4. Release B "Key" System Activities

This section provides descriptions of the key activities of ECS science data processing and system management. The activities are listed in Table 4-1. These activities are the piece parts for the description of the site activities. The activities as described here are site independent, i.e., they describe the way an activity will be performed without site or dataset specifics. The frequency at which the activities or scenarios are performed at a site is provided in Section 5.

Examples of scenarios for each of the key system activities are provided in this section. The three depictions of the scenarios are three views of the scenario. The description provides an overview, the steps provide the man to machine interface, and the figure provides a pictorial representation of the scenario. A list of the scenarios in this section and information regarding whether the scenario is new, modified from Release A, or the same as Release A is provided in Table 4-2. For the scenarios which were in the Operations Concept Document Part 2A, the table also provides the Part 2A section from which the scenario came. A Trouble Ticket and Problem Tracking Scenario is being developed by Release A.

Table 4-1. Release B "Key" System Activities

ACTIVITY	ACTIVITY SECTIONS
4.1 Systems Operations Management Activities	4.1.1 Computer System Administration Activities
	4.1.2 Configuration Management Activities 4.1.3 Fault Management Activities
	4.1.4 Performance Management Activities
	4.1.5 Security and Accountability Activities
	4.1.6 Resource Planning (Scheduling) Activities
	4.1.7 Resource and Logistics Management Activities
	4.1.8 Accounting and Billing Activities
4.2 Science Operations Activities	4.2.1 Science Data Ingest Activities
	4.2.2 Science Data Archival Activities
	4.2.3 Science Data Distribution Activities
	4.2.4 Production Planning Activities
	4.2.5 Production Processing Activities
	4.2.6 User Services Activities
	4.2.7 Science SW Integration and Test Activities
	4.2.8 Information Management Activities
	4.2.9 Science User Activities

Table 4-2. Release B Scenarios (1 of 3)

Part 2B Section	Part 2B Title	Part 2A Section	Part 2A Title	New Mod Same
4.1	**SYSTEMS OPERATIONS MANAGEMENT ACTIVITIES**			
4.1.1	**Computer System Admin. Activities**	**4.1**	**Computer System Admin. Activities**	
4.1.1.1	Comp. Sys. Admin. Backup Scenario	4.1.1	Comp. Sys. Admin. Backup Scenario	Same
4.1.2	**CM Activities**	**4.3**	**CM Activities**	
4.1.2.1	COTS HW Problem Scenario	4.3.1	COTS HW Problem Scenario	Same
4.1.2.2	HW Emergency Change Scenario	4.3.2	HW Emergency Change Scenario	Same
4.1.2.3	COTS SW Problem Scenario	4.3.3	COTS SW Problem Scenario	Same
4.1.2.4	Custom SW Problem Scenario	4.3.4	Custom SW Problem Scenario	Same
4.1.2.5	COTS SW Upgrade Scenario	4.3.5	COTS SW Upgrade Scenario	Same
4.1.2.6	System Enhancement Scenario	4.3.6	System Enhancement Scenario	Same
4.1.3	**Fault Management Activities**	**4.2**	**Fault Management Activities**	
4.1.3.1	Intermittent CPU Failure Scenario	4.2.1	Intermittent CPU Failure Scenario	Same
4.1.3.2	User Notes Performance Degradation Scenario	4.2.2	User Notes Performance Degradation Scenario	Same
4.1.4	**Performance Management Activities**	**4.4**	**Performance Management Activities**	
4.1.4.1	Operations Support Scenario	4.4.1	Operations Support Scenario	Same
4.1.4.2	Preparing for New Algorithm Scenario	4.4.2	Preparing for New Algorithm Scenario	Same
4.1.4.3	Trending Scenario	4.4.3	Trending Scenario	Same
4.1.4.4	Performance Test Generation Request			New
4.1.4.5	Cross DAAC Problem Detection Scenario			New
4.1.5	**Security and Accountability Activity**	**4.5**	**Security and Account'y Mgt. Activ.**	
4.1.5.1	Security Management Scenario	4.5.1	Security Management Scenario	Same
4.1.5.2	Accountability Management Scenario	4.5.2	Accountability Management Scenario	Same
4.1.6	**Resource Planning (Scheduling) Activities**	**4.6**	**Resource Planning Activities**	
4.1.6.1	Planning Production Resources Scenario	4.6.1	Planning Production Resources Scenario	Same
4.1.6.2	Planning Ingest Resources Scenario	4.6.2	Planning Ingest Resources Scenario	Same
4.1.6.3	Schedule Adjudication Scenario			New
4.1.6.4	Bad Data Scenario			New
4.1.7	**Resource and Logistics Management Activities**	4.7	Resource Mgt. and Control Activities	
4.1.7.1	Software Distribution Scenario			New
4.1.7.2	Installation of SW Upgrade	4.7.2	Installation of SW Upgrade	Same
4.1.7.3	Data Processing Host Routine Maintenance Scenario	4.7.1	Data Processing Host Routine Maintenance Scenario	Same
4.1.7.4	Tracking a Corrective Maintenance Action Scenario			New
4.1.7.5	Adding/Updating Inventory Asset Record Scenario			New
4.1.7.6	Cross-DAAC Software Upgrade Coordination Scenario			New
4.1.7.7	Operational System and Test Activity Run in Parallel Scenario			New
4.1.7.8	Mode Management Support Scenario			New
4.1.8	**Accounting and Billing Activities**			
4.1.8.1	Billing and Invoicing a User Scenario			New
4.1.8.2	Receiving and Posting Science User Payments to Accounts Scenario			New

Table 4-2. Release B Scenarios (2 of 3)

Part 2B Section	Part 2B Title	Part 2A Section	Part 2A Title	New Mod Same
4.2	**SCIENCE OPERATIONS ACTIVITIES**			
4.2.1	**Science Data Ingest Activities**	4.8	Science Data Ingest Activities	
4.2.1.1	Automated Network Ingest Scenario	4.8.1	TRMM Level 0 Data Ingest Scenario	Mod
4.2.1.2	Polling Ingest with Delivery Record Scenario	4.8.2		New
4.2.1.3	Polling Ingest without Delivery Record Scenario	4.8.3	TRMM Ancillary Data Ingest Scenario	Mod
4.2.1.4	Hard Media Ingest Scenario	4.8.4	Hard Media Ingest Scenario	Mod
4.2.1.5	Interactive Network Ingest Scenario			New
4.2.1.6	Version 0 Data Ingest Scenario	4.8.5	Version 0 Data Ingest Scenario	Mod
4.2.1.7	Bad Data Scenario			New
4.2.1.8	Document Ingest Scenario			New
4.2.1.9	Document Modification Scenario			New
4.2.2	**Science Data Archival Activities**	4.9	Science Data Archival Activities	
4.2.2.1	Data Insertion Scenario (nominal)	4.9.1	Data Insertion Scenario (nominal)	Mod
4.2.2.2	Data Insertion Scenario (fault)	4.9.2	Data Insertion Scenario (fault)	Mod
4.2.2.3	Data Archive Configuration Maintenance -Media Refresh - Scenario	4.9.3	Data Archive Config. Maint. Scenario (Post Release A Activity)	Mod
4.2.2.4	Data Archive Configuration Maintenance - Lost Volume - Scenario			New
4.2.2.5	Data Type Service Modification Scenario			New
4.2.2.6	Bad Data Scenario			New
4.2.2.7	Data Server Startup/Shutdown Scenario			New
4.2.2.8	ESDT Insert/Delete Scenario			New
4.2.3	**Science Data Distr. Activities**	4.10	Science Data Distr. Activities	
4.2.3.1	Network Data Distribution (Pull) Scenario (nominal)	4.10.1	Network Data Distribution (Pull) Scenario (nominal)	Mod
4.2.3.2	Network Data Distribution (Push) Scenario (nominal)	4.10.2	Network Data Distribution (Push) Scenario (nominal)	Mod
4.2.3.3	Network Data Distribution (Push) Scenario (fault)	4.10.3	Network Data Distribution (Push) Scenario (fault)	Mod
4.2.3.4	Physical Media Distribution Scenario	4.10.4	Hard Media Distribution Scenario	Mod
4.2.3.5	Network Data Distribution (Pull) Scenario (Flood of Requests)			New
4.2.3.6	Network Data Distribution (Push) Scenario (Request from Hell)			New
4.2.3.7	8mm Tape Stacker Distribution Scenario			New
4.2.4	**Production Planning Activities**	**4.11**	Production Planning Activities	
4.2.4.1	Routine Production Planning Scenario	4.11.1	Routine Production Planning Scenario	Mod
4.2.4.2	Replanning Production Scenario	4.11.2	Replanning Production Scenario	Mod
4.2.4.3	On-Demand Request Scenario			New
4.2.4.4	Planning Reprocessing Requests Scenario			New
4.2.4.5	Add Hot Job Scenario			New
4.2.5	**Production Processing Activities**	4.12	Production Processing Activities	
4.2.5.1	Production Processing Job Anomaly Scenario	4.12.1	Production Process. Job Anomaly Scenario	Same
4.2.5.2	Production Process. Job Abnormal Termination Scenario	4.12.2	Production Process. Job Abnormal Termination Scenario	Same
4.2.5.3	Quality Assurance Scenario			New
4.2.6	**User Services Activities**	4.13	User Services Activities	

Table 4-2. Release B Scenarios (3 of 3)

Part 2B Section	Part 2B Title	Part 2A Section	Part 2A Title	New Mod Same
4.2.6.1	Order Tracking Scenario	4.13.1	Order Tracking Scenario	Mod
4.2.6.2	Standard Procedures (Registration) Scenario	4.13.2	Standard Procedures (Login) Scenario	Mod
4.2.6.3	System Status Scenario	4.13.3	System Status Scenario	Mod
4.2.6.4	Place an Order for a Potential User Scenario	4.13.4	Place an Order for a Potential User Scenario	Mod
4.2.6.5	Trouble Ticket Report Scenario	4.13.5	Non-Conformance Report Scenario	Mod
4.2.6.6	Lost User Password Scenario	4.13.6	Lost User Password Scenario	Mod
4.2.6.7	Cross-DAAC Referrals Scenario			New
4.2.7	**Science SW Integ. & Test Activity**	4.14	Science SW Integ. & Test Activity	
4.2.7.1	Transitioning To and From Testing Scenario			New
4.2.7.2	Production Calibration-Validation Scenario			New
4.2.8	**Information Management**			
4.2.8.1	LIM and DIM Schema Maintenance Scenario			New
4.2.8.2	Database Periodic Administration Scenario			New
4.2.8.3	Advertising Review Scenario			New
4.2.8.4	Data Dictionary Valids Ingest - Error Condition - Scenario			New
4.2.8.5	Subscription Event Error Scenario			New
4.2.8.6	Server Saturation Scenario			New
4.2.9	**Science Users**			
4.2.9.1	Simple Search and Order Scenario			New
4.2.9.2	Coincident Search Scenario			New

4.1 System Operations Management Activities

4.1.1 Computer System Administration Activities

System Operations Management Activities are activities that are necessary for System Administration on the local site and system level (SMC). This includes the following;

- system backups
- system restores
- password/account authorization & maintenance
- LAN maintenance
- Internet support
- mail initiation and maintenance
- system help desk functions
- system database/archive management
- system maintenance
- operating system upgrades and installation

System Administration is performed by a combination of COTS software, custom scripts and procedures. The COTS System Administration software package is used to manage configurations of users, desktops, and servers. The System Administration package also facilitates file system management, password/account administration, print management software installations/updates, and trouble ticketing. Backup and Recovery of the unix file system is performed by executing custom scripts developed for ECS. Backup and Recovery of the RDMS is also performed by executing custom scripts. Custom developed scripts are encapsulated into the System Operations Desktop via the System Administration package and can be optionally invoked from a command line or the encapsulated interface. Automatic scheduling of system management scripts during normal system operations is set by the policies and procedures at each site and the SMC. Scripts are scheduled manually as required.

The System Administration package uses a graphical HMI (Human Machine Interface) to interface with the System Administrator using icons, menus and dialog boxes. System administration functions are iconified on the System Operations DeskTop. When system operations personnel want to invoke a system administration function they double click on the icon of the desired function. The System Administrator uses pulldown menus to further select the type of operation they would like to perform. Pop up dialog boxes allowing the System Administrator to input the proper information to perform the System Administrator task. Error checking and consistency checking are performed on operator entries. When necessary the System Administrator can open up a terminal window to invoke system commands using command lines. The Systems Operations Desktop handles proper shutdown of the each of the HMI when Systems Administrator logs off the system.

Due to the wide range of activities included in system administration, many of the activities associated with system administration are included in other sections of this document.

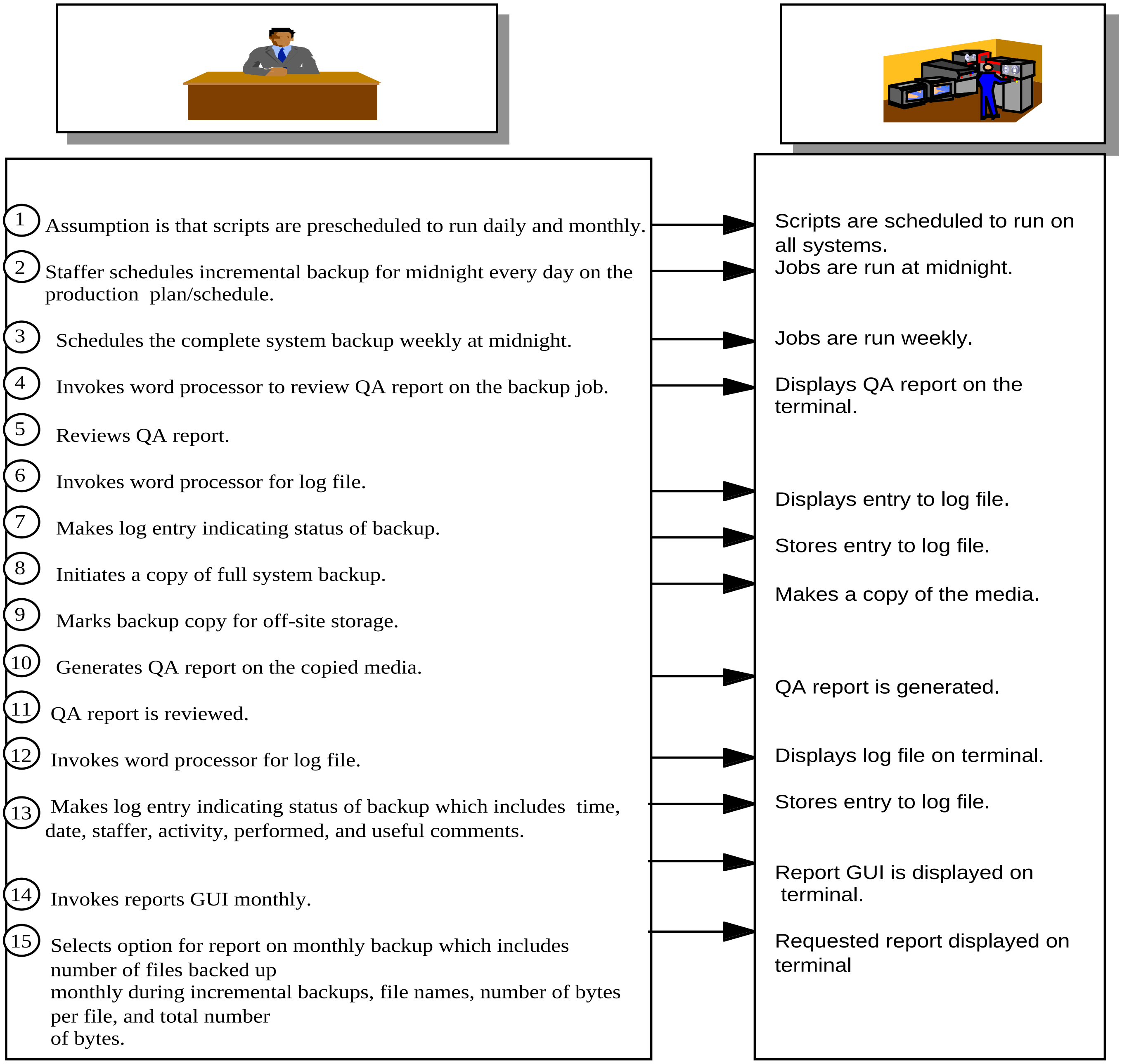
4.1.1.1 Computer Systems Administration Backup Scenario

The general assumption with the backup scenario is that the system will have incremental backups that are run daily, complete backups that are run monthly and that the backup jobs are all run at midnight. The frequency and times that these jobs are run are policy driven and can be different for each DAAC. Also another assumption is that each backup job will contain a QA report for easy analysis.

Figure 4.1.1.1-1 and Table 4.1.1.1-1 depict the activities related to system backup. The system administrator schedules/plans the backup jobs with the resource manager and production manager. These jobs are then run unattended nightly with the complete backup being run once a month.

The system administrator would review the QA report each morning by using the provided word processor to display the text file. If a problem were to occur to the complete backup that is scheduled monthly for example , the administrator may want to reschedule that job as soon as possible. Other problems may require changes in the procedure, for example the time that the job is run. After the jobs have been QAed, the backup is logged in an electronic file using the word processor. This file then could be examined by anyone who wanted information concerning the status of backups or information concerning any problems associated with the backups.

Monthly, the system administrator would invoke the Report Generation GUI to generate reports detailing the backups. The information contained in these reports would include information that would help in future planing of the size and scope of the backup activity.



1 Assumption is that scripts are prescheduled to run daily and monthly.

2 Staffer schedules incremental backup for midnight every day on the production plan/schedule.

3 Schedules the complete system backup weekly at midnight.

4 Invokes word processor to review QA report on the backup job.

5 Reviews QA report.

6 Invokes word processor for log file.

7 Makes log entry indicating status of backup.

8 Initiates a copy of full system backup.

9 Marks backup copy for off-site storage.

10 Generates QA report on the copied media.

11 QA report is reviewed.

12 Invokes word processor for log file.

13 Makes log entry indicating status of backup which includes time, date, staffer, activity, performed, and useful comments.

14 Invokes reports GUI monthly.

15 Selects option for report on monthly backup which includes number of files backed up monthly during incremental backups, file names, number of bytes per file, and total number of bytes.

Scripts are scheduled to run on all systems.

Jobs are run at midnight.

Jobs are run weekly.

Displays QA report on the terminal.

Displays entry to log file.

Stores entry to log file.

Makes a copy of the media.

QA report is generated.

Displays log file on terminal.

Stores entry to log file.

Report GUI is displayed on terminal.

Requested report displayed on terminal

Figure 4.1.1.1-1 Computer Systems Administration Backup Scenario

Table 4.1.1.1-1 Computer Systems Administration Backup Scenario

Step	M&O Staffer	System	Purpose
1	Assumption is made that scripts are prescheduled to run daily and monthly.	Scripts are scheduled to run on all systems.	To collect data automatically.
2	Schedules incremental backup for midnight every day on the production plan/schedule.	Jobs are run at midnight.	To avoid network congestion.
3	Schedules the complete system backup weekly at midnight on the production plan/schedule.	Jobs are run weekly.	Provides complete system backup at regular intervals without tying up hardware resources.
4	Invokes word processor to review the QA report on the backup job where QA report consists of a listing of files with the last update date and time, and scan with dump of first and last file.	Displays QA report on the terminal.	To verify the backup took place without error.
5	Reviews QA report.		Analysis
6	Invokes word processor for log file.	Displays log file on terminal.	To enter backup data on log file.
7	Makes log entry indicating status of backup consisting of time, date, operator, activity performed, and useful comments.	Stores entry to log file.	Log appropriate information on backup.
8	Initiates a copy of full system backup.	Makes a copy of the media.	To have a full system backup copy available.
9	Marks backup copy for off-site storage.		To have an off-site copy of backup in case of emergency.
10	Generates QA report on the copied media.	QA report is generated.	To create a report on the backup.
11	QA report is reviewed.		To verify the backup took place without error.
12	Invokes word processor for log file.	Displays log file on terminal.	To enter backup data on log file.
13	Makes log entry indicating status of backup.	Stores entry to log file.	To store status of backup.
14	Monthly: Invokes reports GUI.	Report GUI is displayed on terminal.	To generate report on backup data.
15	Selects option for report on monthly backup. Report contains the number of files backed up monthly during incremental backups, file names, number of bytes per file, and total number of bytes.	Requested report displayed on terminal.	To view report.

4.1.2 Configuration Management Activities

This section covers the Release B configuration management (CM) process and responsibilities, which are carried over from Release A. Further information on the operational concepts developed for Release A are detailed in the ECS document "ECS Operations Concept for the ECS Project: Part 2A - ECS Release A" (604-CD-003-001, July 1995). Background information (on the various actors involved and the functions performed in the configuration management process) is provided in supplementary documents such as the "Maintenance and Operations Configuration Management Plan for the ECS Project" (102-CD-002-001, September 1995). The scope of CM is limited to control of ESDIS-approved ECS hardware and software resources introduced to the operational environment.

The objective of Configuration Management is to establish and maintain control of the overall ECS systems baseline and implement those changes that will result in the maintenance or enhancement of ECS science user and operational capabilities. The system baseline configuration includes a number of aspects: COTS hardware and software; custom software; science software; database schemas; and related ECS documentation. The ECS configuration process provides for the identification of hardware, software, documentation, and configuration changes.

All custom and COTS software products used in ECS are formally identified in design documents. COTS product specifications in ECS have been documented and approved for use in their respective environments. Deliveries from COTS vendors are accompanied by detailed specifications and complete historical change data. COTS software modified by the vendor is delivered to ECS with addendum documentation describing the changes from the off-the-shelf product and have been added to the baseline as appropriate. Other COTS software changes have been considered and approved/disapproved by ESDIS to define the changes from the off-the-shelf product.

Change requests, change management, and baseline maintenance functions have been approved and are being developed in the Release A design; these will be brought over and used in Release B with little or no changes planned. The respective COTS products used for these functions are: Change Request Manager - PureSoftware's PureDDTS (distributed defect tracking system); Software Change Manager - Atria's ClearCase; and Baseline Manager - HTG's XRP II.

4.1.2.1 COTS Hardware Problem Scenario

In this scenario, depicted in Figure 4.1.2.1-1 and Table 4.1.2.1-1, an operator at the DAAC, EOC, or SMC experiences a problem with his/her workstation (i.e. it crashes). The operator reports the problem either to the system administrator (SA) or by recording the problem into the Trouble Ticketing System (TTS). Assume the operator reports the problem directly to the SA. The SA diagnoses the problem as a system board failure and logs it into the TTS. The maintenance engineer receives the trouble ticket, uses the Baseline Manager to identify the workstation configuration and the responsible maintenance vendor, and calls the maintenance vendor.

The vendor’s maintenance technician arrives and confirms that the system board has failed; replaces the board with an identical board (i.e. same make, model, version); brings the system back up and verifies that the system is operational; and reports the board replacement to the ECS maintenance technician. The site Maintenance Engineer records the time the vendor arrived and departed and actions taken to resolve the problem into the TTS, closes the trouble ticket, and records the serial number of the new board into the property management system.

This scenario did not involve a change to the baselined configuration, therefore no Configuration Change Request (CCR) was generated and no Configuration Control Board (CCB) action was required. Had the repair action resulted in the installation of a part of a different make, model, and/or version from that originally in the workstation, a CCR would have been generated, as presented in the "HW Emergency Change Scenario."

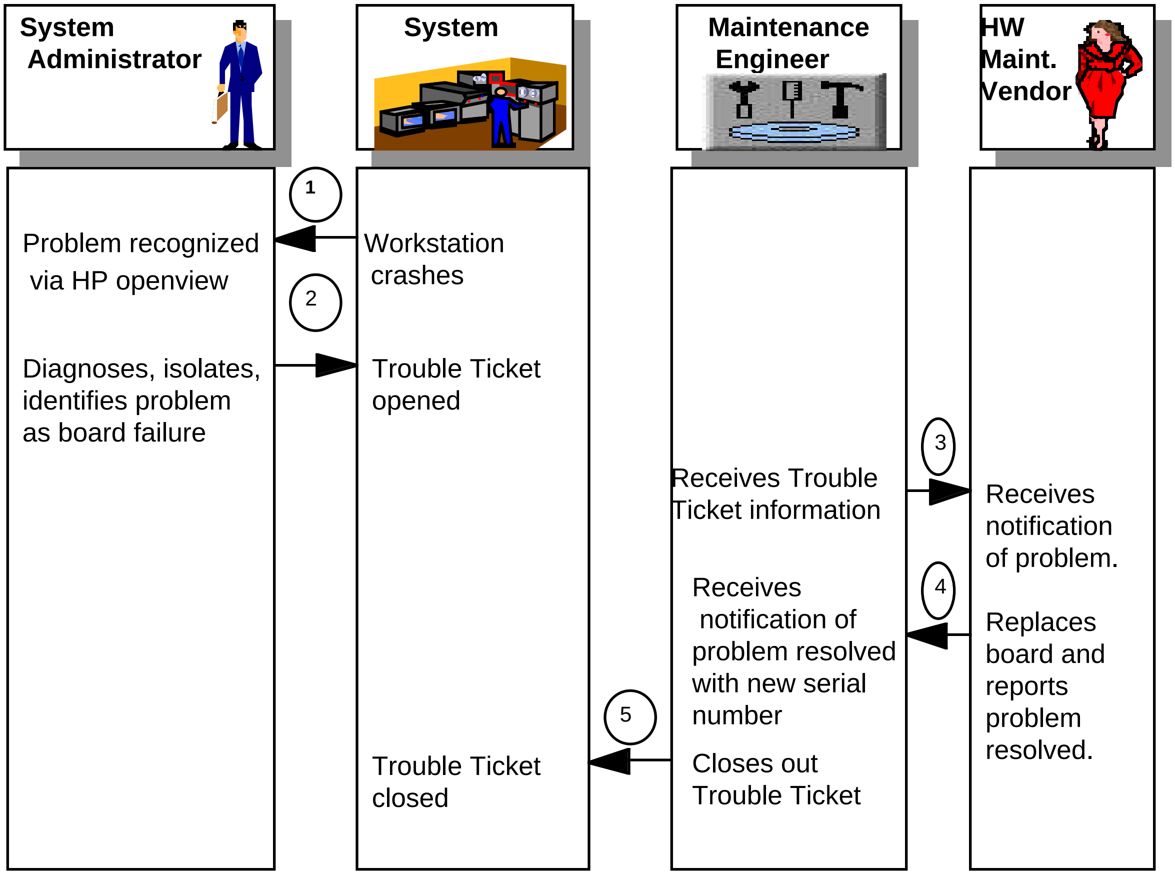

System Administrator
System
Maintenance Engineer
HW Maint. Vendor
1
Problem recognized via HP openview
Workstation crashes
2
Diagnoses, isolates, identifies problem as board failure
Trouble Ticket opened
3
Receives Trouble Ticket information
Receives notification of problem.
4
Receives notification of problem resolved with new serial number
Replaces board and reports problem resolved.
5
Trouble Ticket closed
Closes out Trouble Ticket

Figure 4.1.2.1-1 COTS HW Problem Scenario

Table 4.1.2.1-1 COTS HW Problem Scenario

Steps	Operator/User	System	Purpose
1	Operator workstation crashes, reports problem to Sys. Admin.		HW Problem reported to System Administration.
2	Sys. Admin. diagnoses, isolates, and identifies problem as system board failure, logs Trouble Ticket, sends to Maint. Engr. --- may access B/L Mgr. to assess system configuration to assist in diagnosis/isolation	Records Trouble Ticket	HW Problem diagnosed and identified.
3	Maint. Engr. receives Trouble Ticket and retrieves workstation configuration, runs diagnostics, confirms system board failure, calls HW maint. vendor. Records time called into Trouble Ticket	Trouble Ticket updated with diagnosis and time vendor called	HW Problem maintenance vendor notified of confirmed problem.
4	HW maint. vendor arrives, replaces system board with board of same type and version, tests system, reports problem resolved to Maint. Engr. with serial number of new board.		HW Problem resolved.
5	Maint. Engr. enters maintenance action into Trouble Ticket, closes Trouble Ticket, reports replacement system board serial number into Prop. Mgr.	Maintenance action , vendor arrival and departure time recorded, Trouble Ticket closed. Prop. Mgr. updated with new system board serial number	HW Problem proper information updated.

4.1.2.2 Hardware Emergency Change Scenario

This scenario, depicted in Figure 4.1.2.2-1 and Table 4.1.2.2-1, involves the failure of hardware that requires emergency replacement of a component that is of a later version than is contained in the original equipment in order to bring a system back into operation.

This scenario is at 7PM on a Saturday evening. The operator has detected a problem with the automated tape library (ATL) and reported the problem to the Trouble Ticketing System (TTS). The trouble ticket is routed to the System Administrator, who confirms that the system will not operate and notifies the site Maintenance Engineer. After running further diagnostics, the Maintenance Engineer reports the problem and symptoms to the OEM's maintenance desk. The

OEM maintenance representative arrives and concludes that a controller card has failed. The only card the OEM has immediately available is of a later version and no spares are available on site. It will be Monday at the earliest before a replacement board of the same revision level can be located. The site maintenance engineer reports this to the operations Crew Chief (i.e. shift leader) for a decision.

The DAAC cannot afford to have the ATL down until Monday. The Crew Chief calls the DAAC manager at home, apprises him of the situation, and obtains approval to replace the board with the later version if tests conclude that it works properly. The OEM's maintenance representative installs the board. The site's Sustaining Engineers tests the new controller board, find that it works properly, and bring the ATL back on line. The Sustaining Engineer generates a CCR to document the configuration change and the authority for the change. The site Maintenance Engineer records the replacement action in the TTS, references the related CCR, and closes the trouble ticket. The site Maintenance Engineer updates the property record with the model, version, and serial number of the new board.

The site CM Administrator reviews the CCR, determines whether it requires review by the site CCB, and updates the Baseline Manager with the new configuration and CCR # authorizing the change. The CCR is also reviewed by the ECS SEO to assess whether there may be impacts to the ECS and/or applicability to other sites. The ESDIS CCB is provided an information copy of the CCR for their review and concurrence.

In the event that it is later discovered that the new version controller board has adverse impacts when operating in the ECS configuration, a board of the original version will have to be obtained to replace the newer version. In such case, the action will be recorded on a new CCR, referencing the previous CCR.

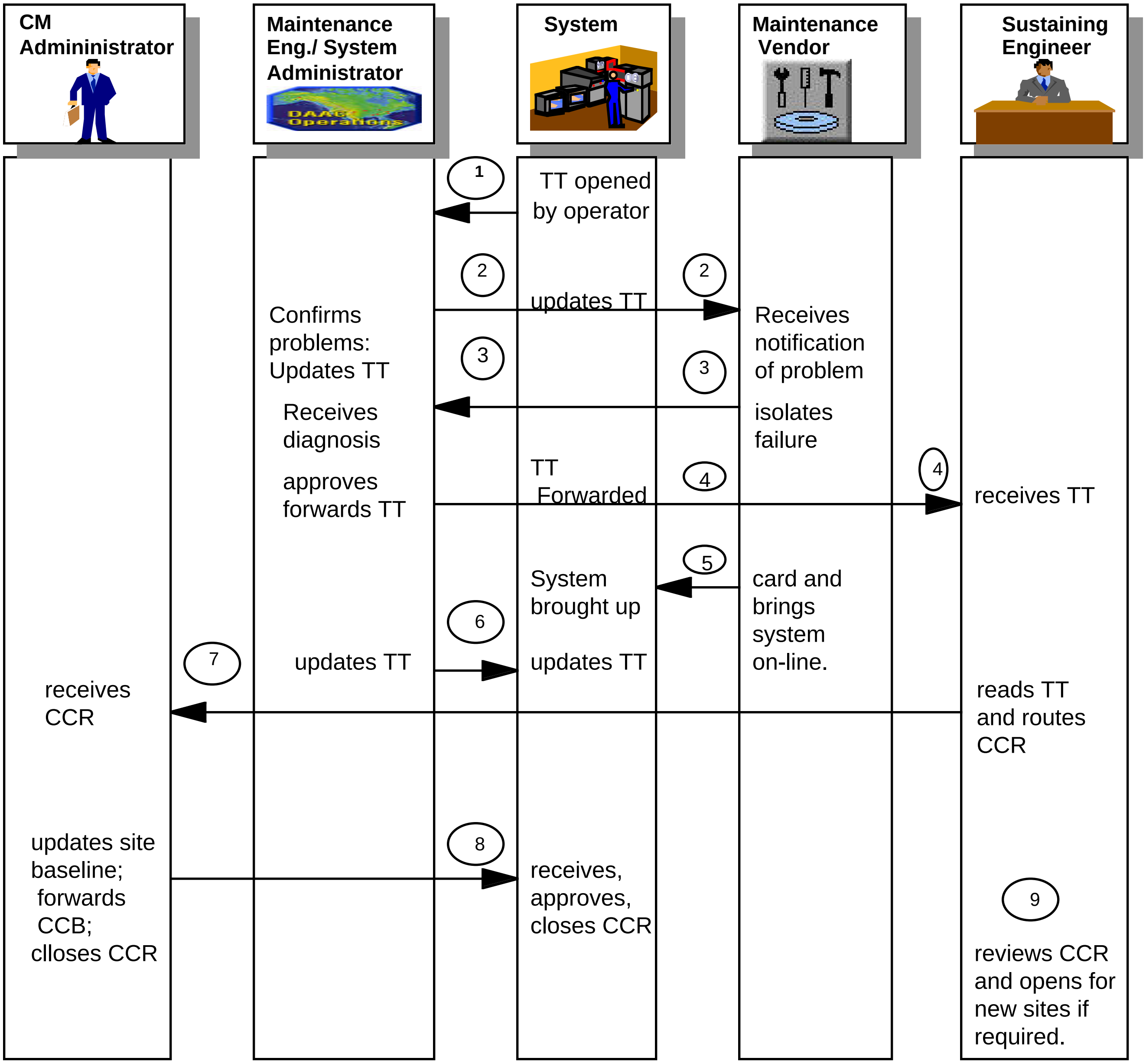


Figure 4.1.2.2-1 HW Emergency Change Scenario

Table 4.1.2.2-1 HW Emergency Change Scenario

Steps	Operator/User	System	Purpose
	Normal Scenario:		
1	Operator prepares Trouble Ticket to report ATL controller failure	Trouble Ticket recorded	Hardware failure reported.
2	Sys. Admin. and Maint. Engr. confirm ATL controller failure, call ATL maintenance vendor, report call and time in Trouble Ticket	Diagnosis and vendor call recorded in Trouble Ticket	Hardware failure confirmed vendor notified.
3	Maintenance vendor isolates failure to the controller card. Later version card is the only card available.		Failure isolated.
4	Crew Chief notified of situation and decision needed to bring ATL up to full operating capability. Approves use of the newer version card, records decision in Tbl. Tkt., forwards Tbl. Tkt. to Sust. Engr.		Crew Chief notified. Newer equipment approved.
5	Maintenance vendor installs card, tests using HW diagnostics. Crew chief authorizes controller to be brought back on line.		New equipment installed and authorized.
6	Maint. Engr. records card installation by mode/version into the Trouble Ticket.	Trouble Ticket action recorded.	Trouble Ticket updated.
7	Sust. Engr. reads Tbl. Tkt. and prepares for discussion into the Trouble Ticket.	Install action recorded in CCR. CCR routed to the CM Admin.	CCR generated by SE.
8	CM Admin. updates site baseline, forwards the CCR to the CCB, and when CCB approves the action, closes the CCR	Site ATL baseline updated in B/L Mgr. CCR closed.	Site baseline updated and CCR closed by CCB.
9	SEO reviews emergency CCR, checks for applicability to other sites, opens new CCR if other sites require change		CCR reviewed for other sites.

4.1.2.3 COTS Software Problem Scenario

This scenario, depicted in Figure 4.1.2.3-1 and Table 4.1.2.3-1, involves a problem with COTS SW that is maintained by commercial SW developer (i.e. IDL Corporation).

A user reports a problem with the IDL visualization SW to the site's User Services Desk. The User Services Desk records the information and opens a Trouble Ticket in the TTS. (NOTE: If an ECS operator notices the problem, he/she reports the problem by opening the Trouble Ticket). The Trouble Ticket is routed to the site Sustaining Engineer(s) for diagnosis. The Sustaining Engineer verifies that the visualization SW creates a error code each time a series of commands is executed, and reports it to the commercial SW developer's Help Line. The developer has had previous reports of the problem from other customers and has developed a patch to resolve it. The Sustaining Engineer is told that the patch is available on the Internet, who then retrieves the patch. (NOTE: The site Sustaining Engineer has the option, since this SW is used at all sites, to forward the Trouble Ticket to the ECS SEO for resolution. In this case, he has taken the problem on at the site level.)

The site Sustaining Engineer tests the patch and verifies that it solves the problem and does not conflict with other ECS applications. The Sustaining Engineer prepares a CCR using Change Request Manager, recommending that the patch be approved for installation at the site. The CCR is forwarded by the site's CM Administrator to the Site CCB and to the ECS SEO. The SEO retrieves the patch, conducts further testing, and concludes that the problem affects all sites. The SEO forwards the CCR to the other sites for their comments, recommending that the ESDIS CCB approve the patch for installation at all sites. The ESDIS CCB reviews the DAAC assessments in making its decision. The ESDIS CCB may direct that the patch be installed at all sites, selected sites, not at all, or leave it to the option of the individual DAACs. The CCB may also establish a schedule in which the installations must be accomplished or leave it up to the DAACs to determine the schedule.

When approved by the ESDIS CCB, the patch is provided to all sites, tested by the site Sustaining Engineer (optional), and installed by the site's System Administrator. Any site having an open Trouble Ticket associated with the patch will close its Trouble Ticket once the patch is installed. The site System Administrator reports installation of the patch to the site's CM Administrator, who updates the Baseline Manager and records completion of the CCB-directed installation in the Change Request Manager. Once all sites report installation of the patch, the ECS System Administrator closes the CCR and reports closure in the next status report to the ESDIS CCB.

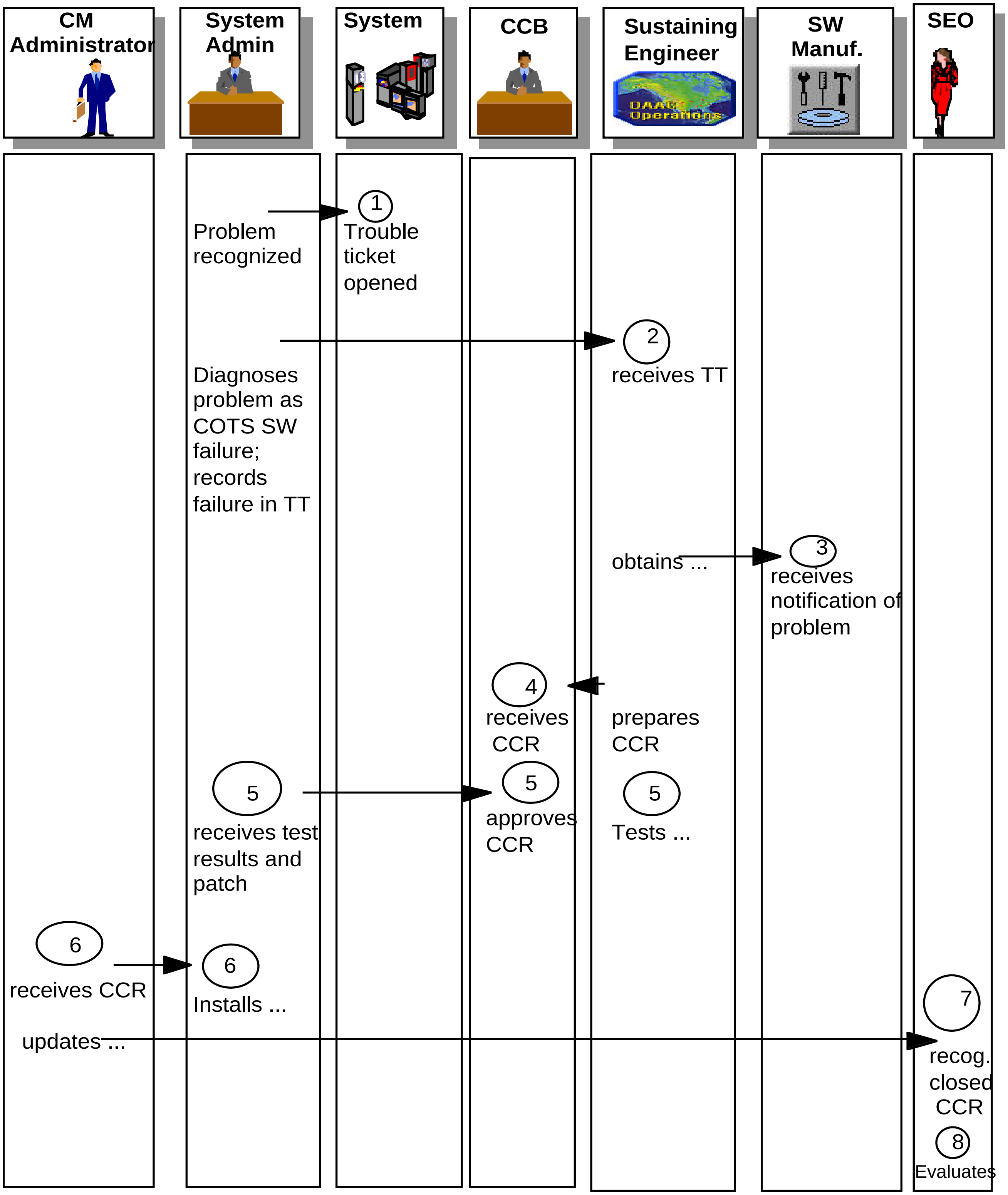


Figure 4.1.2.3-1 COTS SW Problem Scenario

Table 4.1.2.3-1 COTS SW Problem Scenario

Steps	Operator/User	System	Purpose
1	Operator reports problem as a Trouble Ticket	Operator Trouble Ticket recorded	Software problem reported.
2	Sys. Admin. diagnoses the problem as a failure in the COTS SW, records diagnosis in the Trouble Ticket, forwards Trouble Ticket to the Sust. Engr.	Trouble Ticket updated with diagnosis	Problem diagnosed and recorded.
3	Sust. Engr. reports problem to SW manufacturer Help Desk, obtains patch (if available), and records vendor-provided solution in Trouble Ticket. Note: If vendor does not have a patch for the problem, it will either 1) develop a patch (if urgent) or 2) correct the problem in a subsequent release (most likely case).	Solution recorded in the Trouble Ticket	SW manufacturer notified.
4	Sust. Engr. prepares CCR to obtain approval to apply the patch.	CCR generated in CR Mgr.	CCR prepared for patch approval.
5	Upon receipt of CCB approval, Sust. Engr. tests patch, verifies that it corrects the problem and is compatible, and forwards test results and patch to the Sys. Admin.	CCB approval recorded in CR Mgr.	Patch tested and approved.
6	Sys. Admin. installs the patch, records action taken on the Trouble Ticket, records completion on the CCR, and routes CCR to the CM Admin.	Action taken recorded on Trouble Ticket Install recorded on the CCR	Patch installed.
7	CM Admin. updates site baseline and closes CCR.	Site baseline updated in B/L Mgr. CCR closed	CCR closed after site baseline updated.
8	SEO evaluates whether patch should be applied at other sites. If so, SEO generates new CCR for site review and ESDIS approval		Other sites reviewed for patch.

4.1.2.4 Custom Software Problem Scenario

This scenario, depicted in Figure 4.1.2.4-1 and Table 4.1.2.4-1, involves a problem (not an enhancement) with custom SW developed by the ECS Science and Communications Development Organization (SCDO) and maintained by the SEO.

A science user reports a problem with one of the ECS toolkits to the site’s User Services Desk. The User Services Desk records the information and opens a Trouble Ticket in the TTS. (If an ECS operator notices the problem, he/she reports the problem by opening the Trouble Ticket.) The Trouble Ticket is routed to the site Sustaining Engineer(s) for diagnosis. The Sustaining Engineer verifies that the toolkit’s interface to another ECS application (either custom or COTS) does not provide the desired results and identifies the source statements that are in error. The Sustaining Engineer estimates that it will take one man month to correct and test the application and generates a CCR recommending that the ECS SEO perform the work. The site CCB reviews the CCR and concurs that it be forwarded to the SEO for resolution. (NOTE: The site CCB has the option to develop the fix at the site with its Sustaining Engineering staff or to forward the

CCR to the ECS SEO for resolution, since the SW is used at all sites). If the site Sustaining Engineer develop the fix, the ESDIS CCB would still have to approve installation of the fix at the site and determine whether and when it should be installed at all sites.

The ECS CM Administrator receives the CCR and forwards it to the SEO for assessment and recommendation. Using ClearCase (the SW CM System), the SEO, confirms the problem, solution, and resources required to do the work. It determines that the problem is serious enough to fix now, rather than incorporate into a future release, and recommends to the SEO develop the SW change and implement across all DAACs. (NOTE: The SEO and SCDO could decide that the change should be developed by SCDO, rather than the SEO, because of the nature of the change, affect on development work, or work loads). The DAACs review the CCR and provide their impact assessments and recommendations to the ESDIS CCB. The ESDIS CCB directs that the change be developed by the SEO and installed at all DAACs on a specified date, during a specific window, or by a specific date.

The SEO develops, compiles, tests, and distributes the new SW version according to the CCB-directed schedule. The new version is entered into ClearCase. The site's Sustaining Engineer tests (optional) and the Systems Administrator installs the change. Sites having an open Trouble Ticket associated with the fix close their Trouble Ticket once the patch is installed. The site System Administrator reports installation of the new version to the site's CM Administrator, who updates the Baseline Manager and records completion of the installation in the Change Request Manager. Once all sites report installation of the patch, the ECS System Administrator closes the CCR and reports closure in the next status report to the ESDIS CCB.

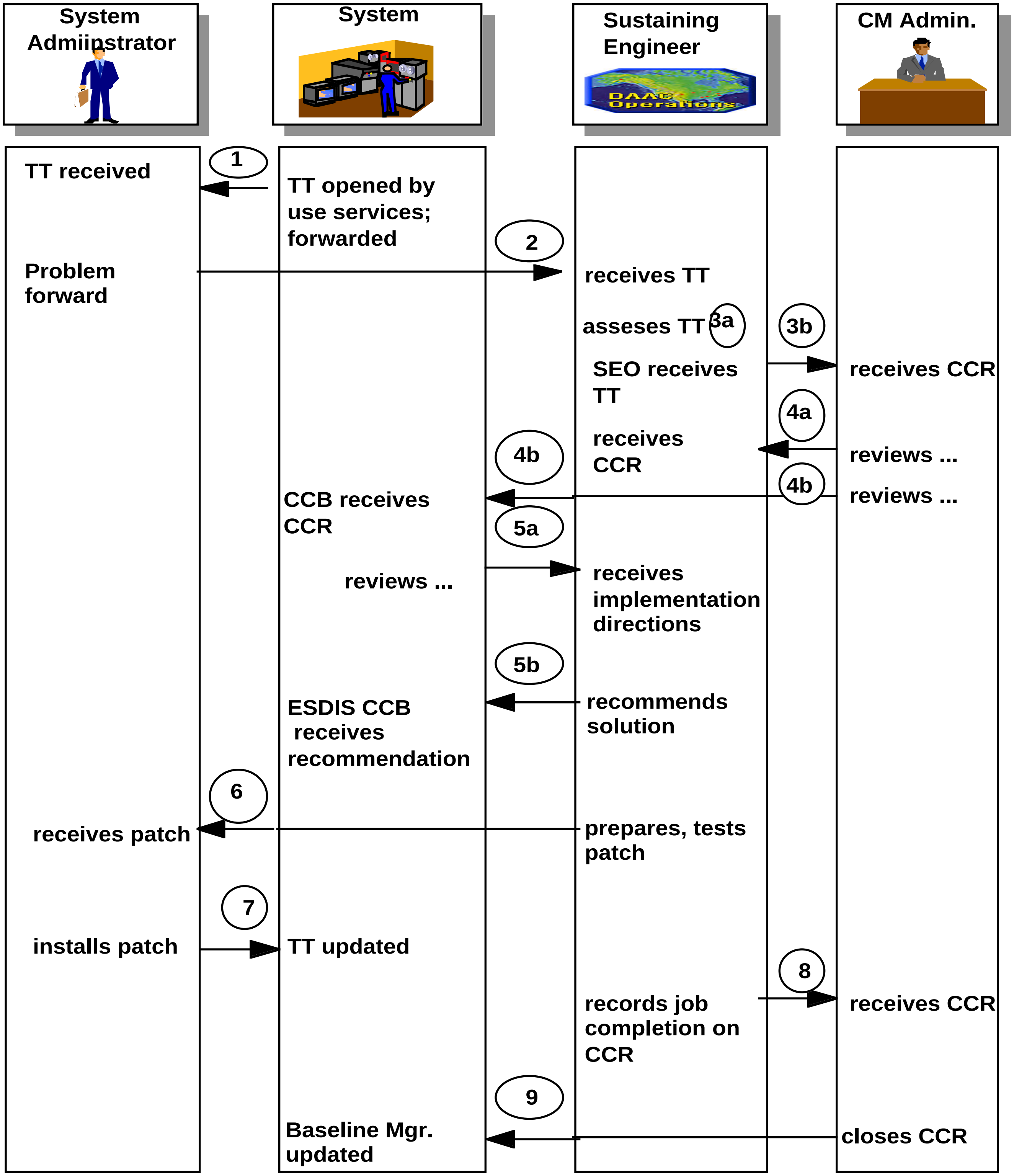


Figure 4.1.2.4-1 Custom SW Problem Scenario

Table 4.1.2.4-1 Custom SW Problem Scenario

Steps	Operator/User	System	Purpose
1	User reports problem to User Services Desk, which opens Trouble Ticket Operator reports problem by completing Trouble Ticket.	Trouble Ticket recorded and forwarded to System Administrator	Record problem
2	Systems Administrator confirms problem is with the custom SW, records diagnosis on the Trouble Ticket, and forwards Trouble Ticket to the Sustaining Engineer.	CCR record established in CR Manager.	Confirm problem
3	Sustaining Engineer assesses problem, determines whether the action belongs to the site or the SEO. If an SEO action, forwards Trouble Ticket to SEO. If site action, prepares CCR, provides proposed solution with impacts, schedules, and resource assessment.	CCR record established in CR Manager.	Assess problem and prepare CCR if necessary
4	CM Administrator reviews for CCB review or sends to SEO for action.	CCR provided to CCB members or SEO, as applicable.	Forward reviewed CCR
5	If site CCB action, CCB reviews, decides, and provides implementation directions to the Sustaining Engineer. If SEO action, SEO recommends solution to ESDIS CCB for decision.	CCB decision recorded in CCR	CCB decision
6	SW patch is prepared by the site Sustaining Engineer, SEO, or the ECS Development Org (as applicable). Once developed and tested, the patch is provided to site System Administrator for installation at sites.	Development status recorded in CCR	Develop and test the solutions; install solution
7	After site testing System Administrator installs the patch, and records completion on the Trouble Ticket.	Install action recorded on Trouble Ticket and Trouble Ticket closed	close Trouble Ticket
8	Site CM Administrator closes in CCR when SW patch installed,	Install recorded in CCR	update CCR
9	Site CM Administrator closes CCR and records B/L change in B/L Manager	CCR Closed, reported in next status report, B/L Manager updated with SW change to all platforms/ sites in which patch is applied	close CCR and record

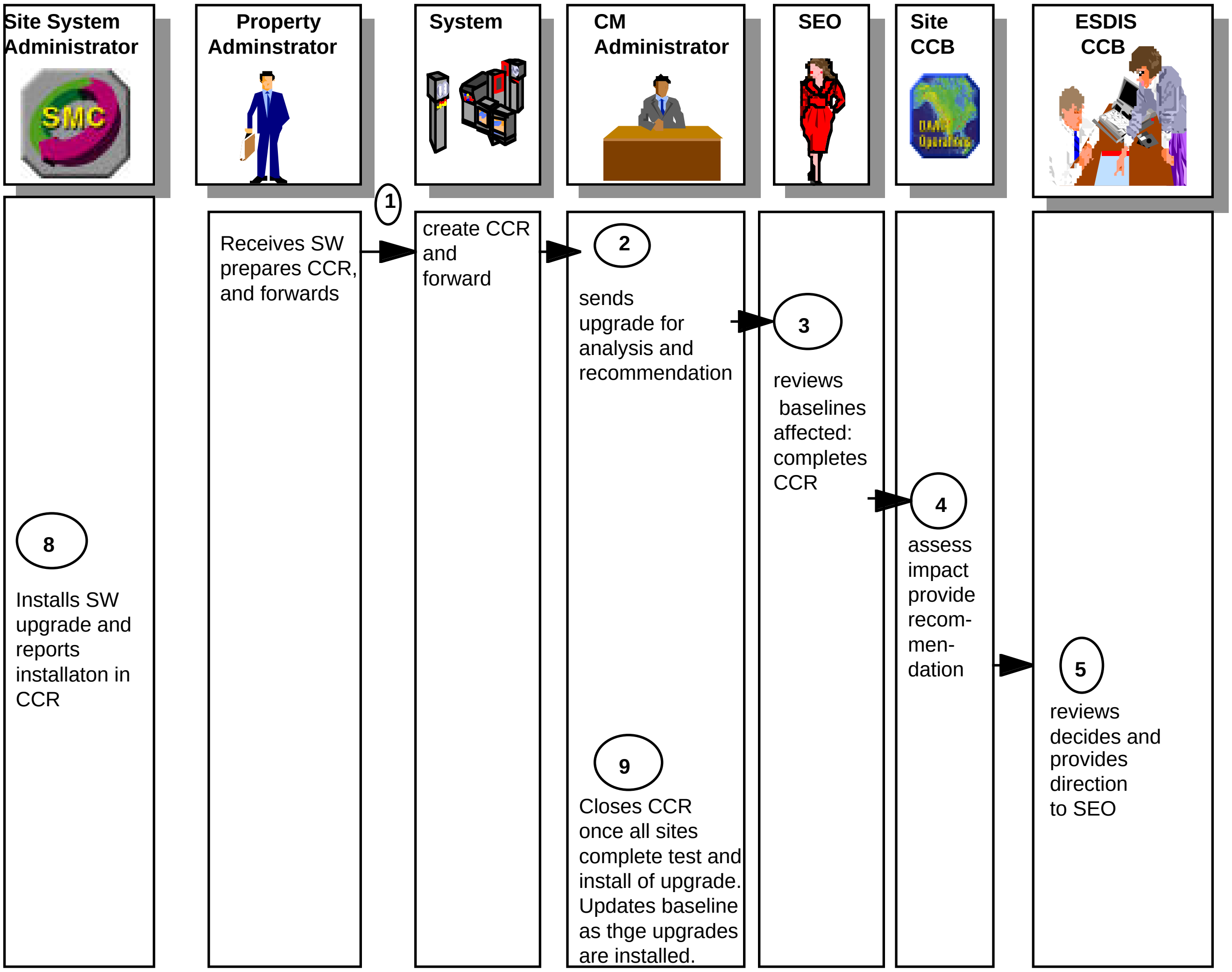
4.1.2.5 COTS Software Upgrade Scenario

This scenario, depicted in Figure 4.1.2.5-1 and Table 4.1.2.5-1, addresses the upgrade of an ECS COTS application developed by the commercial developer.

The ECS Property Administrator receives an upgrade to Scheduler, (a COTS SW application), records the receipt in the Property Management System, and prepares a CCR announcing the upgrade. (NOTE: All COTS SW upgrades are shipped by the vendor to the ECS Property

Administrator, rather than to the sites, to ensure vendor compliance with their contracts and to ensure compatibility of COTS versions with other ECS applications). The CCR is forwarded to the SEO, which assesses applicability system-wide and impacts to other ECS applications and resources; tests the upgrade; and prepares a recommendation. Meanwhile, the sites review the CCR and forward their impact assessments for ESDIS CCB decision.

The ESDIS CCB directs that the COTS SW upgrade be installed at all DAACs not later than a specified date. The site's Sustaining Engineer tests (optional) and the Systems Administrator installs the upgrade and reports installation to the site's CM Administrator, who updates the Baseline Manager and records completion of the installation in the Change Request Manager. Once all sites report installation of the upgrade, the ECS System Administrator closes the CCR and reports closure in the next status report to the ESDIS CCB.



Site System Administrator
SMC
Property Adminstrator
System
CM Administrator
SEO
Site CCB
ESDIS CCB
1
Receives SW prepares CCR, and forwards
create CCR and forward
2
sends upgrade for analysis and recommendation
3
reviews baselines affected: completes CCR
4
assess impact provide recom-men-dation
5
reviews decides and provides direction to SEO
8
Installs SW upgrade and reports installaton in CCR
9
Closes CCR once all sites complete test and install of upgrade. Updates baseline as thge upgrades are installed.

Figure 4.1.2.5-1 COTS SW Upgrade Scenario

Table 4.1.2.5-1 COTS SW Upgrade Scenario

Step	Operator/User	System	Purpose
1	ECS Prop. Admin. receives COTS SW upgrade, prepares receiving report, prepares CCR, forwards CCR to ECS CM Admin.	CCR recorded in CR Mgr. SW receipt recorded in Prop. Mgr.	Receive upgrade and prepare CCR
2	ECS CM Admin. sends upgrade to SEO for analysis, and recommendation		Analysis of upgrade
3	SEO review B/Ls affected by the upgrade, completes CCR analysis and recommendations, and forwards CCR to sites for recommended change impact analysis	CCR forwarded to sites	Perform change impact analysis
4	Site CCBs assess impacts of SEO proposed action, provide recommendation to ESDIS CCB		Site's to provide recommendation to ESDIS CCB
5	ESDIS reviews CCR and SEO and site recommendation. Decides and provides implementation directions to SEO/Sites		Provide direction
6	ECS CM Admin. records CCB decision	CCB decision recorded in CCR	Record decision
7	SEO takes action necessary to implement the upgrade	Implementation status recorded in CCR as it occurs	Implement decision
8	Site Sys. Admin. installs SW upgrade and reports installation in the CCR	CCR completion recorded	Install SW upgrade
9	ECS CM Admin. closes CCR once all sites complete test and install of the upgrade. Site CM Admin. updates site B/L as the upgrades are installed	Site B/Ls updated in B/L Mgr	Close CCR

4.1.2.6 System Enhancement Scenario

This scenario, depicted in Figure 4.1.2.6-1 and Table 4.1.2.6-1, addresses the flow of a system enhancement proposed by a science user or DAAC operator.

A science user calls the User Services Desk suggesting an enhancement to one of the ECS custom toolkits that will enable users faster, more direct access to data products. The User Services Desk records the suggestion on a Trouble Ticket and forwards the Trouble Ticket to the site Sustaining Engineer. The Sustaining Engineer assesses the feasibility, impacts, and resources required, and prepares a CCR with recommendation to the site CCB. The site CCB reviews the assessment and recommendations and takes one of the following actions:

1. If not feasible because of impacts or resource requirements, disapproves the CCR. In such cases, the Sustaining Engineer will report back to the Science User or operator the reasons why it was disapproved and close the Trouble Ticket and CCR.

2. If DAAC unique, disapproves and close the CCR and Trouble Ticket, or approve for DAAC development and implementation. DAAC unique modifications to ECS applications must be forwarded to the SEO for assessment and ESDIS CCB for approval. If approved, the site Sustaining Engineers will develop and maintain the enhancement.

3. If not DAAC unique and feasible, forwards the CCR with assessment and recommendation to the SEO. The SEO will evaluate the suggested enhancement, provide impacts and resource assessments, and provide a recommendation to the ESDIS CCB for decision.

ESDIS CCB-approved enhancements may be developed by the SEO or by the ECS development organization (i.e. SCDO), depending on workloads, release schedules, and functionality. Enhancements may be developed for delivery with a future ECS release or may be delivered between major releases (unlikely).

When development and testing are completed, the site’s Systems Administrator installs the new SW version. The site CM Administrator updates the site’s Baseline Manager with the new version information and reports its installation in the Change Request Manager. Once all sites report installation of the new version, the ECS System Administrator closes the CCR and reports closure in the next status report to the ESDIS CCB.

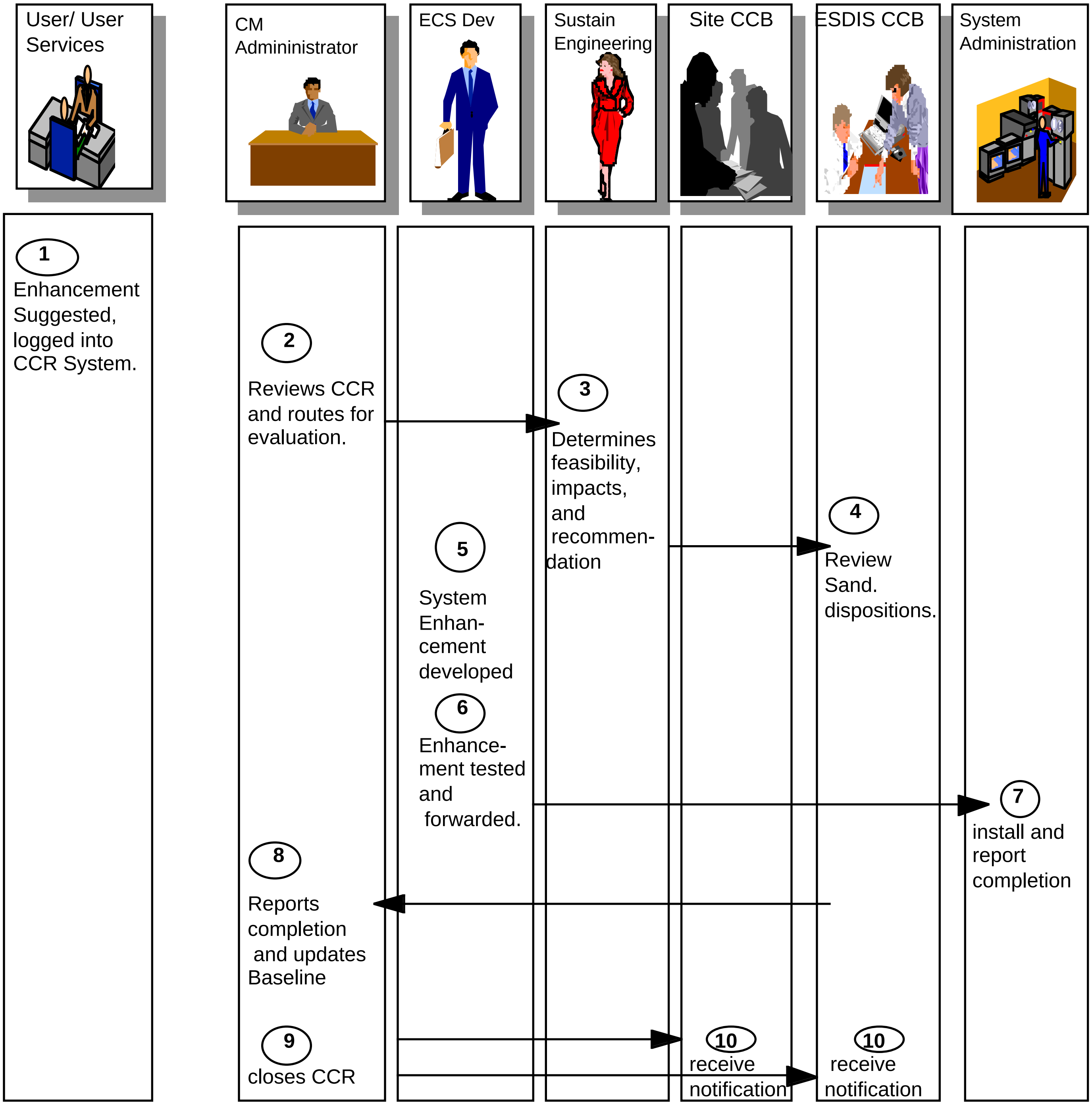

User/ User Services
CM Admininistrator
ECS Dev
Sustain Engineering
Site CCB
ESDIS CCB
System Administration
1
Enhancement Suggested, logged into CCR System.
2
Reviews CCR and routes for evaluation.
3
Determines feasibility, impacts, and recommen- dation
4
Review Sand. dispositions.
5
System Enhan- cement developed
6
Enhance- ment tested and forwarded.
7
install and report completion
8
Reports completion and updates Baseline
9
closes CCR
10
receive notification
10
receive notification

Figure 4.1.2.6-1 System Enhancement Scenario

Table 4.1.2.6-1 System Enhancement Scenario

Step	Operator/User	System	Purpose
1	User suggests system enhancement to the User Svc. Desk. User Svcs. logs the proposed enhancement into the CCR system. If suggested by a site operator, the operator will enter the information into the CCR	CCR recorded established in CR Mgr.	Log proposed enhancement into CCR system
2	Site CM Admin. reviews CCR for completeness and routes to site Sust. Engr. for evaluation		Review and forward
3	Sust Engr. determines feasibility, impacts, and recommendation. If site specific, the CCR is dispositioned by the site CCB. If relevant to the system, the SEO prepares feasibility and impact assessment and forwards to ESDIS CCB with recommendations	B/L Mgr. reviewed to assist in assessment of applicability and impacts	Determine feasibility, impacts, and recommendation
4	ESDIS CCB reviews SEO and site CCB recommendations, then dispositions the CCR. If approved, implementation directions are provided.	Decision recorded in CCR	Determine disposition of CCR
5	System enhancements will be developed by the SEO or the ECS development organization, depending on the nature of the change and distribution of work at the time	SW enhancement development uses SW Change Mgr. to control changes to the SW	Enhancement development
6	Once developed and tested, the enhancement is forwarded to the sites for installation by the site Sys. Admin.		forward to sites for installation of enhancement
7	Site Sys. Admin. will install the enhancement and report completion to the site CM Admin.	CCR updated to reflect installation	installation of enhancement
8	Site CM Admin. reports completion to the Sys. CM Admin. and updates the site B/L.	B/L Mgr. updated to reflect changes in site baselines	Baseline updated
9	System CM Admin. closes the CCR when all sites have completed the installation	CCR closure reported in CR Mgr.	CCR closed
10	ESDIS/Site CCBs are notified when CCR is completed and closed via CCR Status Report		notification of closure

4.1.3 Fault Management Activities

Fault management addresses the detection and notification of faults associated with the following:

- Network devices
- Hosts and peripherals
- Operating Systems
- Process monitoring
- Applications

Fault management for the ECS system is performed by COTS and custom software tools and by users reporting problems either electronically or manually to the trouble ticketing system. Software tools include local management agents residing on the individual hardware and software components of the ECS system. The primary fault management tools are the COTS products HP OpenView and Tivoli. Fault management software provides automatic fault detection through the use of visual or audible notifications such as Pop-up window alerts or Icons changing color on the management console. A COTS trouble ticketing package provides a means for users to input fault information detected independent of the automated fault detection process. Fault isolation and diagnosis is supporter by tools such as a fault log browser, customized test procedures using HP Openview and Tivoli and vendor diagnostic tests. The system provides help in the automatic diagnosis of system faults and provides alerts to the system manager whenever possible. Once a fault has been isolated and diagnosed by either automatic or manual means, procedures are invoked to provide recovery from the fault. Automated recovery from common faults is provided by pre defined scripts. Fault management includes the ability to monitor and to stop and restart ECS host application. All faults are recorded and documented in system log files for further evaluation and analysis.

Fault management uses the SNMP (Simple Network Management Protocol) standard with predefined MIB (Management Information Base) objects. MIB objects provide values for system metrics such as network traffic and error counts. Fault monitoring is accomplished by configuring graphical network maps, scripts, Management Agent traps and by setting monitoring parameters, thresholds and collections frequencies. The configuration of each item is specified by site specific policies and procedures. HP Open View and Tivoli provide a GUI to build maps, set up profiles for monitoring parameters, setting thresholds and frequencies and executing scripts. Monitoring can be performed on the console device, system log files and system parameters defined by MIB object values. System status is represented by color coded map icons that can be drilled down to lower level of detail. MIB object values can be monitored and set from the system console. The setting of MIB objects provides direct remote operator control of the ECS system and allows applications to be shut down or restarted.

The ECS network, hosts and host applications are monitored for faults. Faults are also detected by SNMP Management Agents supplied by hardware vendors for communication devices on the network (bridges, routers, hubs, gateways). SNMP Management Agents MIBs are loaded into the Fault Management Application HP Open View. Custom SNMP Agents add the ability to detect faults within applications by using an applications MIB and provide the means to shutdown and restart application software. Proxy Management agents interface with non SNMP agents supplied by software vendors such as Sybase. The Management Agents are controlled/configured via Tivoli to send information to the Fault Manager.

If a management agent detects an error it sends a trap to the fault manager which provides a alert. Alerts are configurable to be audible, to be visual (by changing the color of the icon corresponding to the ECS resource), to activate a pager, to write a trouble ticket, etc. Error messages are logged and displayed in the event browser window with diagnostic information on the error. Faults can be manually identified and isolated by browsing events through an event browser GUI.

4.1.3.1 Intermittent CPU Failure Scenario

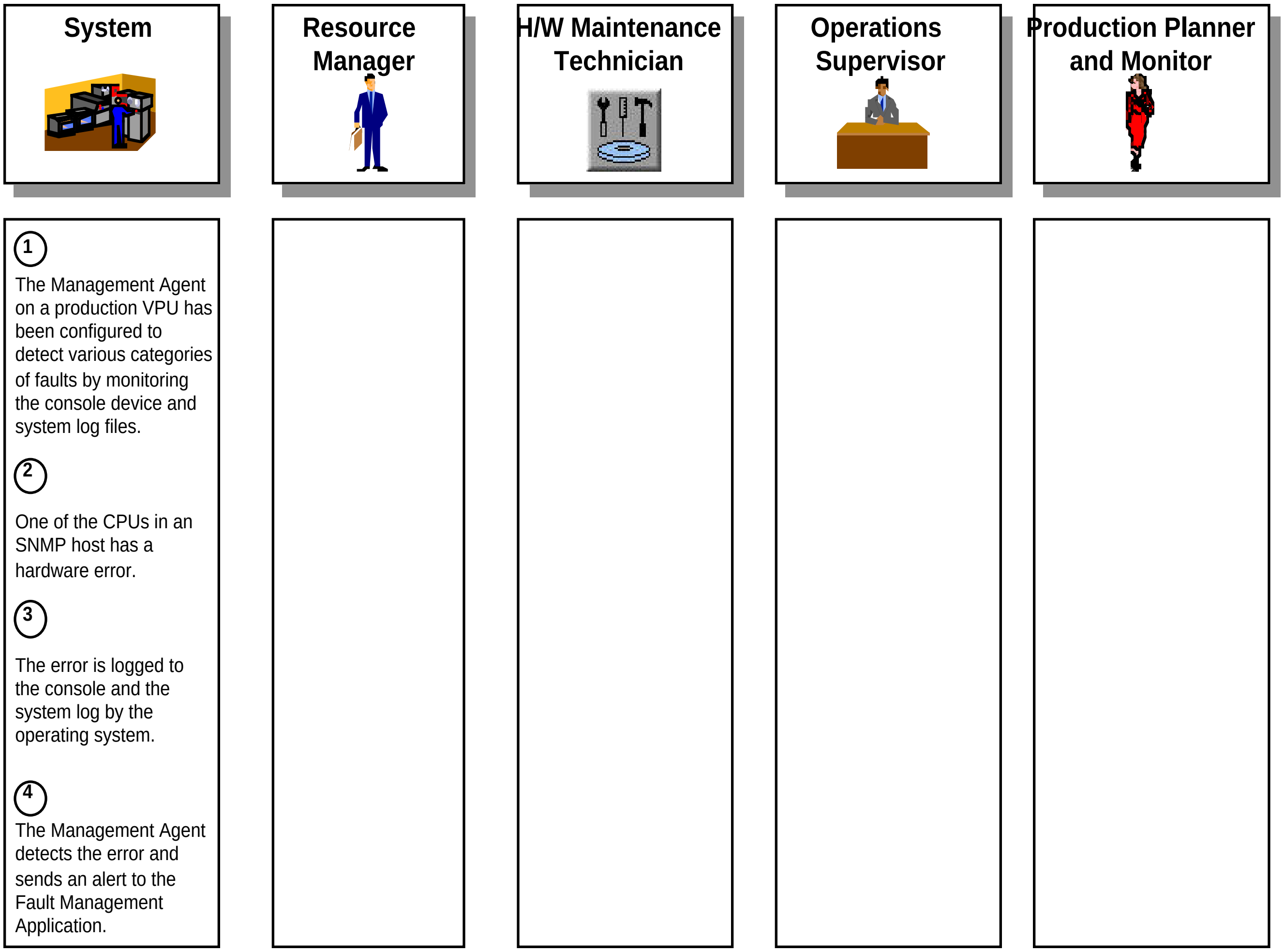
The assumption made for this scenario, depicted in Figure 4.1.3.1-1 and Table 4.1.3.1-1, is that there is a maintenance contract established with the vendor of the Symmetric Multiprocessing (SMP) host in question (the primary/critical production system) to respond for corrective maintenance in no more than four hours of a call being placed.

In setting up for fault detection, the Management Agent on the main production CPU (SMP) is configured to detect various categories of faults, including hardware errors (CPU, Memory, peripherals), by monitoring the console device and system log files. One of the CPUs in an SMP (Symmetric Multiprocessing) host (the primary/critical production system) has a hardware error, which is logged to the console and the system log by the operating system. The Management Agent detects the error and sends an alert to the Fault Management Application which provides a notification to the Resource Manager (RM) via an audible alert and by changing the color of the icon corresponding to the host. Further, an error message is logged and displayed in the event browser window with diagnostic information on the error. A Trouble Ticket is opened by the RM, who logs the system Id, time of occurrence (for RMA (MDT, MTTR, MTBF) purposes), and assigns it to the Hardware Maintenance Technician (HMT). The RM is then able to isolate the nature of the fault by browsing through the event browser window, and by browsing through the logfile, is able to determine that there have been no other related hardware errors logged. The RM updates the TT with the time, his/her initials and findings, and assigns the TT to the HMT. The HMT calls the vendor, describes the nature of the fault, and logs a service call. The vendor confirms that a spare CPU board for the SMP host is in the inventory.

The RM apprises the Operations Supervisor of the situation. Since the host supports Production, the Production Planner and Monitor (PPM) are also informed of the situation, who then, with the RM approve one hour down time for the CPU swap. The PPM suspend all new production jobs, and determine the host can not be brought down now since a rerun would take 12 hours, and that the three jobs currently running would likely complete in four hours, based on the fact that one CPU is not available

The assumption at this point is that it is determined that recovery of the production backlog is possible even with the delay; therefore the jobs are not rescheduled.

The HMT updates the Trouble Ticket with the scheduled down time (i.e., to indicate the “wait” time so as to allow MDT to be accurately computed). The vendor is informed of the schedule to shutdown, who then arrives at the appointed time with the replacement CPU board. The production jobs 20 minutes more than expected after which the system is shut down, the CPU board replaced, diagnostics run, and the system rebooted within an hour from the originally scheduled time. The total down time for the host is 30 minutes. The HMT updates the Trouble Ticket to enter information for down time, and changes the status of the Trouble Ticket to “Closed”. The Production Monitor then resumes the production tasks held in the production queue for this host. Based on the information in the Trouble Ticket, the accurate calculation of MDT of the host, the MTBF and the MTTR the CPU board, by the Performance Management Application facilitated.



1

The Management Agent on a production VPU has been configured to detect various categories of faults by monitoring the console device and system log files.

2

One of the CPUs in an SNMP host has a hardware error.

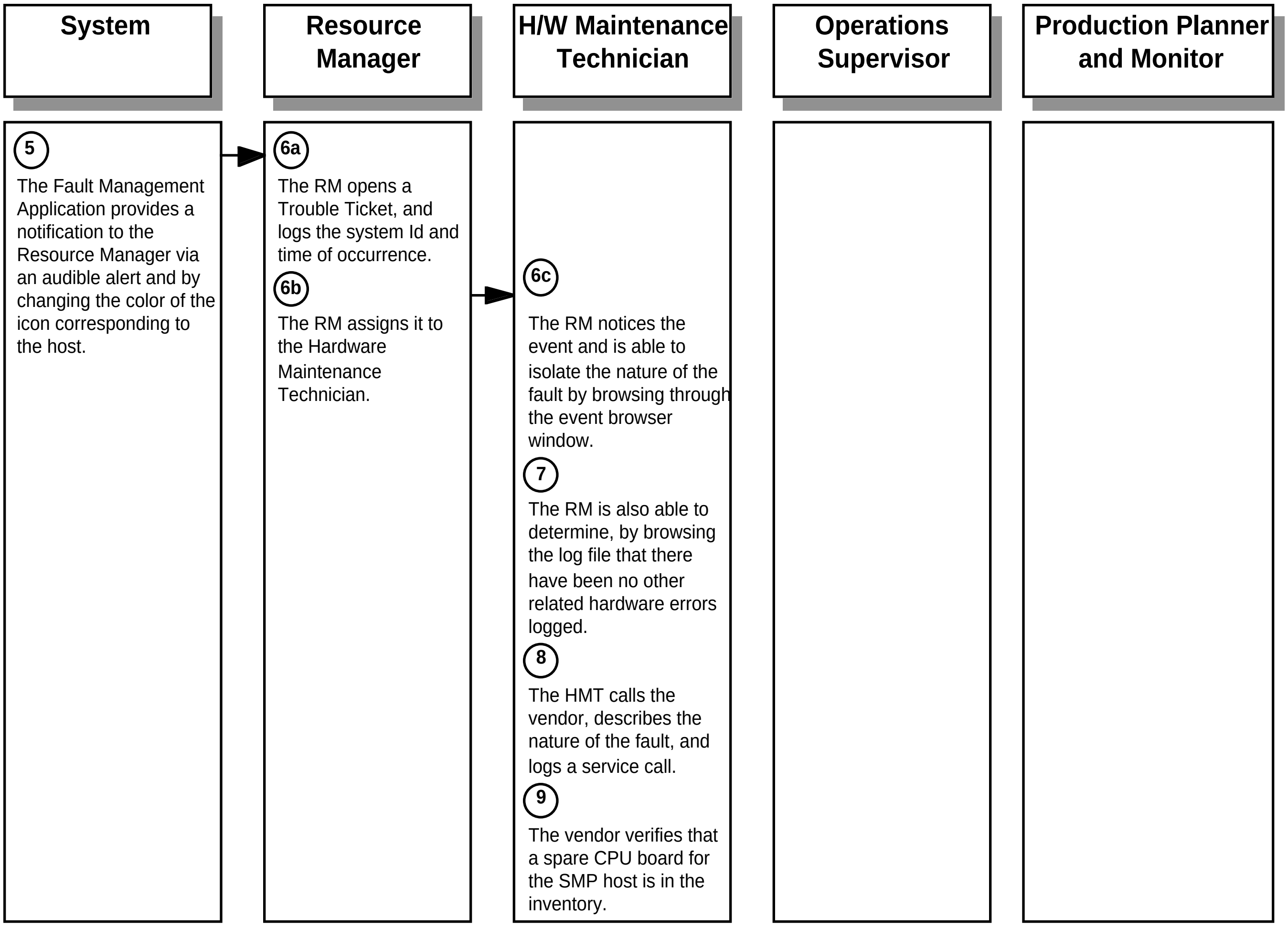
3

The error is logged to the console and the system log by the operating system.

4

The Management Agent detects the error and sends an alert to the Fault Management Application.

Figure 4.1.3.1-1 Intermittent CPU Failure Scenario (1 of 3)



5 The Fault Management Application provides a notification to the Resource Manager via an audible alert and by changing the color of the icon corresponding to the host.

6a The RM opens a Trouble Ticket, and logs the system Id and time of occurrence.

6b The RM assigns it to the Hardware Maintenance Technician.

6c The RM notices the event and is able to isolate the nature of the fault by browsing through the event browser window.

7 The RM is also able to determine, by browsing the log file that there have been no other related hardware errors logged.

8 The HMT calls the vendor, describes the nature of the fault, and logs a service call.

9 The vendor verifies that a spare CPU board for the SMP host is in the inventory.

Figure 4.1.3.1-1 Intermittent CPU Failure Scenario (2 of 3)

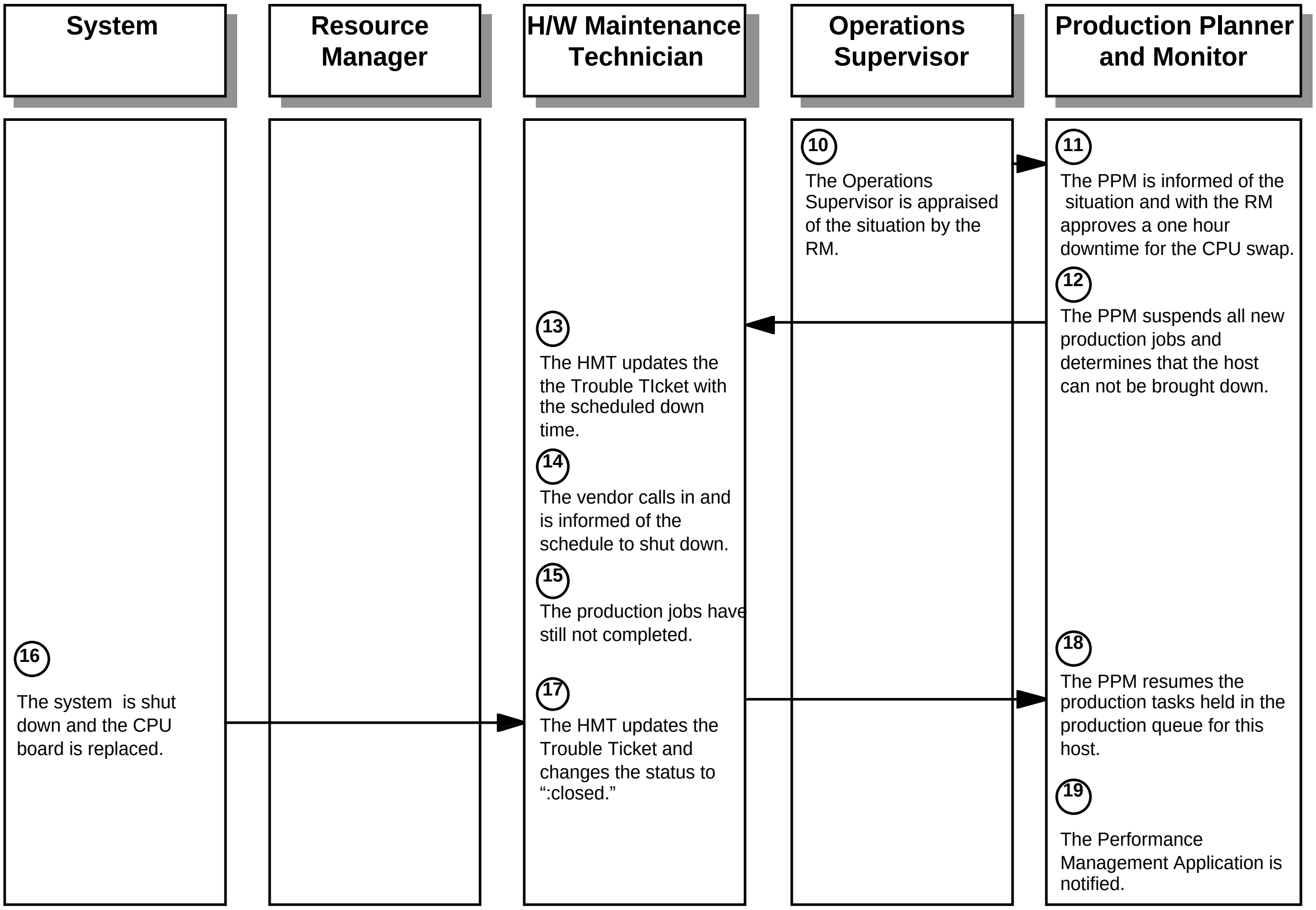

System
Resource Manager
H/W Maintenance Technician
Operations Supervisor
Production Planner and Monitor
10
The Operations Supervisor is appraised of the situation by the RM.
11
The PPM is informed of the situation and with the RM approves a one hour downtime for the CPU swap.
12
The PPM suspends all new production jobs and determines that the host can not be brought down.
13
The HMT updates the the Trouble TIcket with the scheduled down time.
14
The vendor calls in and is informed of the schedule to shut down.
15
The production jobs have still not completed.
16
The system is shut down and the CPU board is replaced.
17
The HMT updates the Trouble Ticket and changes the status to “:closed.”
18
The PPM resumes the production tasks held in the production queue for this host.
19
The Performance Management Application is notified.

Figure 4.1.3.1-1 Intermittent CPU Failure Scenario (3 of 3)

Table 4.1.3.1-1. Intermittent CPU Failure Scenario (1 of 3)

Step	System	Data Exchanged	Human Actions	Purpose
1	The management Agent on a production VPU has been configured to detect various categories of faults, including hardware errors (CPU, Memory, peripherals), by monitoring the console device and system log files.			Fault detection
2	One of the CPUs in an SMP (Symmetric Multiprocessing) host (the primary/ critical production system) has a hardware error			
3	The error is logged to the console and the system log by the operating system			To account for error
4	The Management Agent detects the error and sends an alert to the Fault Management Application			To alert Fault Manageme nt Application and Resource Manager
5	The Fault Management Application provides a notification to the Resource Manager (RM) via an audible alert and by changing the color of the icon corresponding to the host. Further, an error message is logged and is played in the event browser window with the details of the error	Visual, audible Notifications		
6a			The RM opens a Trouble Ticket, logs the system Id, time of occurrence (for RMA (MDT, MTTR, MTBF) purposes)	Record keeping and work load delegation
6b			The RM assigns it to the Hardware Maintenance Technician (HMT)	
6c			The RM notices the event, and is able to isolate the nature of the fault by browsing through the event browser window	

Table 4.1.3.1-1. Intermittent CPU Failure Scenario (2 of 3)

Step	System	Data Exchanged	Human Actions	Purpose
7			The RM is also able to determine, by browsing through the log file that there have been no other related hardware errors logged	Determine if other hardware errors were logged
8			The HMT calls the vendor, describes the nature of the fault, and logs a service call	Record keeping
			The HMT calls the vendor, describes the nature of the fault, and logs a service call	Contact vendor
9			The vendor verifies that a spare CPU board for the SMP host is in the inventory	
10			The Operations Supervisor is apprised of the situation by the RM	To notify appropriate personnel
11			Since the host supports Production, the Production Planner and Monitor (PPM) are informed of the situation, who then, with the RM approve on hour down time for the CPU swap	To approve downtime for CPU
12			THe PPM suspend all new production jobs, and determine the host can not be brought down now since a rerun would take 12 hours, and that the three jobs currently running would likely complete in four hours, based on the fact that one CPU is not available ASSUMPTION: It is determined that recovery of the production backlog is possible even with the delay; therefore the jobs are not rescheduled	

Table 4.1.3.1-1. Intermittent CPU Failure Scenario (3 of 3)

Step	System	Data Exchanged	Human Actions	Purpose
13			The HMT updates the Trouble Ticket with the scheduled down time (i.e., to indicate the "wait" time so as to allow MDT to be accurately computed)	Record keeping
14			The vendor calls in, and is informed of the schedule to shutdown	Keep vendor appraised of situation
15			The production jobs have still not completed. They take 20 minutes more than expected. Everyone waits till the job run through to completion	
16			The system is shut down, the CPU board replaced, diagnostics run, and the system rebooted within an hour from the originally scheduled time. Total host down time is 30 minutes	
17			The HMT updates the Trouble Ticket to enter information for down time, and changes the status of the Trouble Ticket to "Closed"	To change status of TT
18			The Production Monitor then resumes the production tasks held in the production queue for this host	Resume normal operations
19			Based on the information in the Trouble Ticket, the accurate calculation f MDT of the host, the MTBF and the MTTR the CPU board, by the Performance Management Application facilitated	Notify Performanc e Manageme nt Application

4.1.3.2 User Notes Performance Degradation Scenario

This scenario, depicted in Figure 4.1.3.2-1 and Table 4.1.3.2-1, deals with a user experiencing performance degradation problems several times in using a service at a DAAC while logged in from his SCF. The scenario shows how with the use of the Trouble Ticketing capabilities, problem resolution histories are maintained for ready reference, and how the resolution process is expedited.

A user calls User Services (US) to report bad response time of the system. The US person opens a Trouble Ticket (TT), enters information about the user (Name, location, telephone number, email address, and a description of the problem - particularly the transaction that had the response time), which in this case happened to be a Search in the Advertising Service. The US person gives the user a reference TT number.

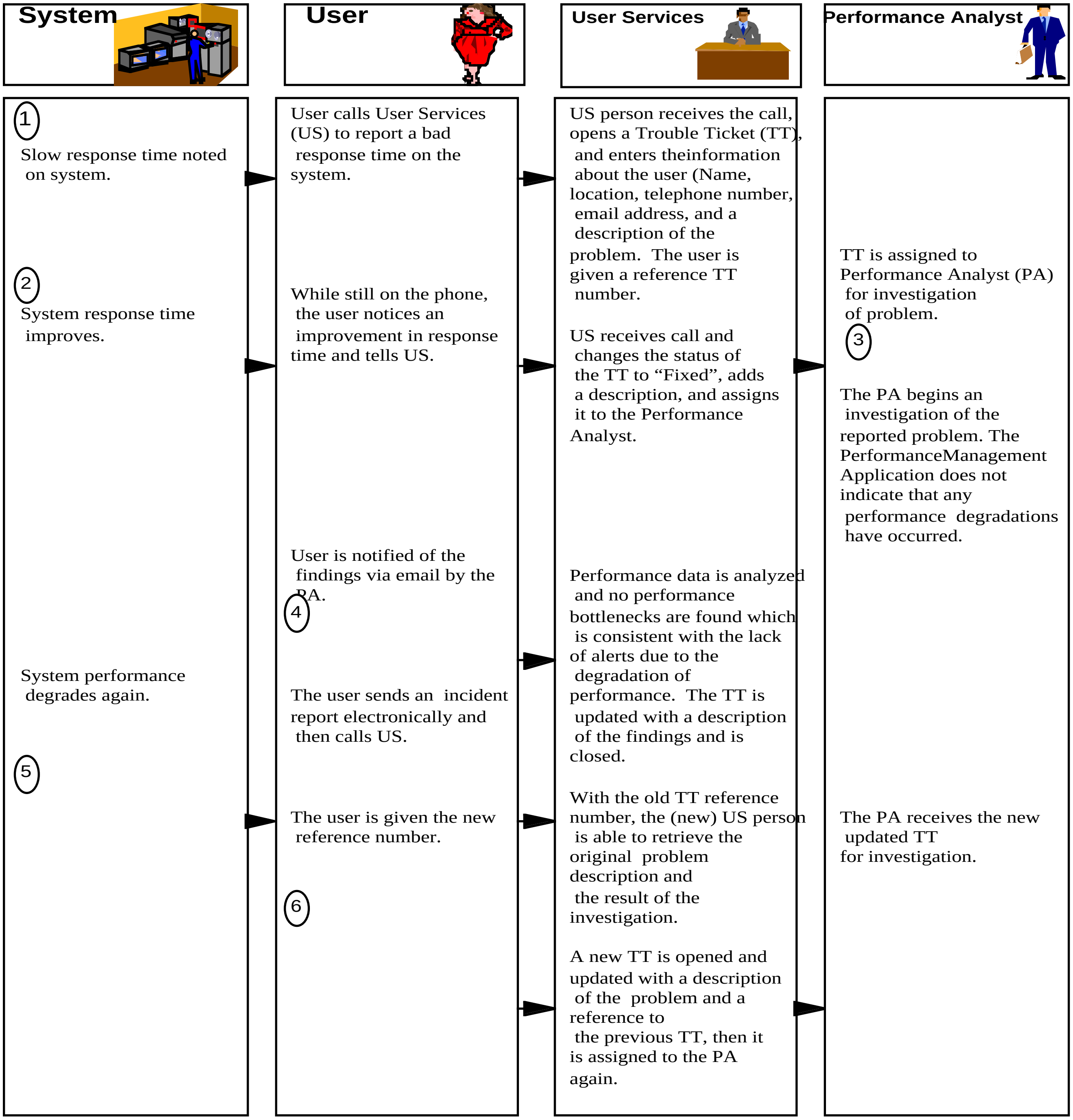
While still on the phone, the user notices an improvement in response time, and tells the US so. The US person changes the status of the TT to “Fixed”, adds a description, and assigns it to the Performance Analyst (PA). The US person also tells the user to call again with the reference number in case the problem reoccurs.

The PA begins an investigation of the reported problem. The performance data examined does not reveal any performance bottlenecks, which is consistent with the lack of alerts due to degradation of performance. The PA then updates the TT with a description of the findings, closes it, and the notifies the user of the findings via email.

The problem reoccurs on a different day, the user sends an incident report electronically, and then calls US with the old TT reference number. The (new) US person is able to retrieve the original problem description and the result of the original investigation. A new TT is opened, updated with a description of the problem and a reference to the previous TT, and assigned again to the PA. The user if informed of the new reference number. As in the first instance, performance improves during the conversation, and the user informs the US person. The TT is updated and assigned the status “Fixed”, but is not closed.

The PA investigates the issue again, come up with the same results as before, and it is suggested to the user that the problem may be at the user’s end, and that the user’s Systems Administrator (SA) be contacted to look into the problem. The user’s SA looks at performance data for the user’s host, finds CPU utilization normal, and indicates that there is no performance problem on the user’s side.

The problem occurs a third time, and the user calls the US with the old TT reference numbers. A new TT is opened and assigned to the PA as before, who then contacts the user’s SA. The analysis of the data at the user’s network for the three time intervals that the user has reported problems indicates that while network and the user’s host show normal utilizations, the highest level of activity on the LAN was between the user’s host and the local archive server. It is found that this traffic was due to data being transferred during a test run of an algorithm being developed by the user. The local SA then loads a more granular performance management product on the user’s host, and with the user, recreates the scenario, while collecting performance data. This reveals that the network adapter on the user’s host is the performance bottleneck (low bandwidth), “choking” when the data transfer for the algorithm occurred. This was found to coincide with the time the user tried to access the Advertising Service. The SA then informs the user and the personnel at the DAAC, based on which, the TT at the DAAC is updated with the analysis & resolution and closed.



Slow response time noted on system.

System response time improves.

System performance degrades again.

User calls User Services (US) to report a bad response time on the system.

While still on the phone, the user notices an improvement in response time and tells US.

User is notified of the findings via email by the PA.

The user sends an incident report electronically and then calls US.

The user is given the new reference number.

US person receives the call, opens a Trouble Ticket (TT), and enters theinformation about the user (Name, location, telephone number, email address, and a description of the problem. The user is given a reference TT number.

US receives call and changes the status of the TT to “Fixed”, adds a description, and assigns it to the Performance Analyst.

Performance data is analyzed and no performance bottlenecks are found which is consistent with the lack of alerts due to the degradation of performance. The TT is updated with a description of the findings and is closed.

With the old TT reference number, the (new) US person is able to retrieve the original problem description and the result of the investigation.

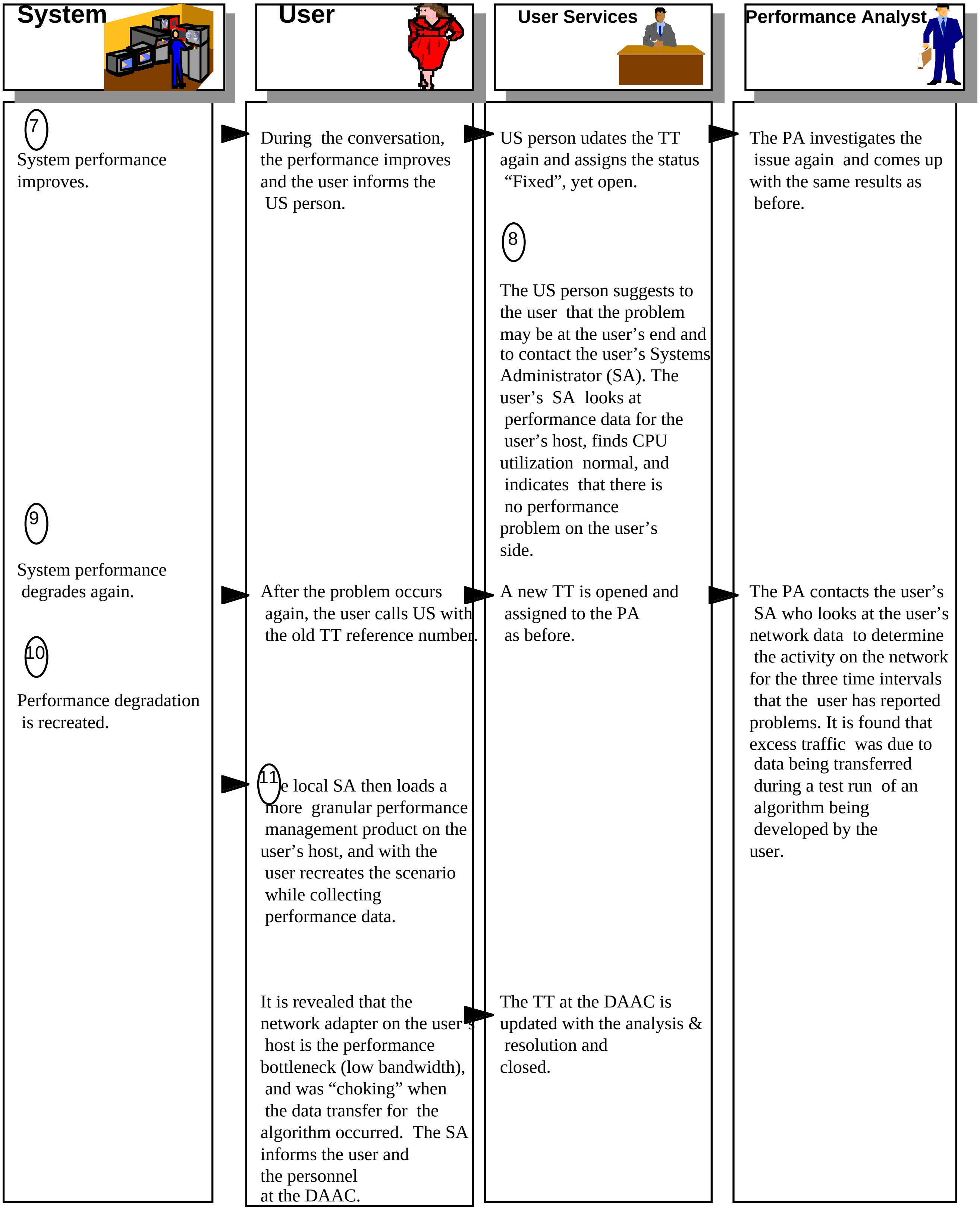
A new TT is opened and updated with a description of the problem and a reference to the previous TT, then it is assigned to the PA again.

TT is assigned to Performance Analyst (PA) for investigation of problem.

The PA begins an investigation of the reported problem. The PerformanceManagement Application does not indicate that any performance degradations have occurred.

The PA receives the new updated TT for investigation.

Figure 4.1.3.2-1 User Notes Performance Degradation Scenario (1 of 2)



7

System performance improves.

9

System performance degrades again.

10

Performance degradation is recreated.

During the conversation, the performance improves and the user informs the US person.

After the problem occurs again, the user calls US with the old TT reference number.

11 e local SA then loads a more granular performance management product on the user’s host, and with the user recreates the scenario while collecting performance data.

It is revealed that the network adapter on the user’s host is the performance bottleneck (low bandwidth), and was “choking” when the data transfer for the algorithm occurred. The SA informs the user and the personnel at the DAAC.

US person udates the TT again and assigns the status “Fixed”, yet open.

8

The US person suggests to the user that the problem may be at the user’s end and to contact the user’s Systems Administrator (SA). The user’s SA looks at performance data for the user’s host, finds CPU utilization normal, and indicates that there is no performance problem on the user’s side.

A new TT is opened and assigned to the PA as before.

The TT at the DAAC is updated with the analysis & resolution and closed.

The PA investigates the issue again and comes up with the same results as before.

The PA contacts the user’s SA who looks at the user’s network data to determine the activity on the network for the three time intervals that the user has reported problems. It is found that excess traffic was due to data being transferred during a test run of an algorithm being developed by the user.

Figure 4.1.3.2-1 User Notes Performance Degradation Scenario (2 of 2)

Table 4.1.3.2-1 User Notes Performance Degradation Scenario (1 of 3)

Step	System	User	User Services	Performance Analyst	Purpose
1	Slow response time noted on system.	User calls User Services (US) to report a bad response time on the system.	The US person receives the call, opens a Trouble Ticket (TT), and enters information about the user (Name, location, telephone number, email address, and a description of the problem - particularly the transaction that had the response time). This transaction happens to be a Search in the Advertising Service. The US person gives the user a reference TT number.		To inform User Services of system performance degradation.
2	System response time improves.	While still on the phone, the user notices an improvement in response time and tells US.	Receives call and changes the status of the TT to "Fixed", adds a description, and assigns it to the Performance Analyst. The US person also tells the user to call again with the reference number in case the problem reoccurs.	TT is assigned to Performance Analyst (PA) for investigation of problem.	To begin an investigation of the problem.
3				The PA begins an investigation of the reported problem. The Performance Management Application does not indicate that any performance degradations have occurred. The network path the user used to connect to the DAAC (Client Subsystem and Interoperability (Advertising) Services) from SCF is determined.	To investigate the problem.
4		User is notified of the findings via email by the PA.	Performance data is analyzed, and no performance bottlenecks are found which is consistent with the lack of alerts due to the degradation of performance. The Trouble Ticket is updated with a description of the findings and is closed.		To determine the cause of the problem and clear up the Trouble Ticket.
5	System performance degrades again.	The problem occurs on a different day, the user sends an incident report electronically and then calls US.	With the old TT reference number, the (new) US person is able to retrieve the original problem description and the result of the investigation.		To inform User Services of recurring problem.
6		The user is given the new reference number.	A new TT is opened and updated with a description of the problem and a reference to the previous TT then assigned again to the PA.	Receives new updated TT for investigation.	Start a new investigation.

Table 4.1.3.2-1 User Notes Performance Degradation Scenario (2 of 3)

Step	System	User	User Services	Performance Analyst	Purpose
7	System performance improves.	During the conversation, the performance improves and the user informs the US person.	US person updates the TT again and assigns the status "FIxed", yet open.	The PA investigates the issue again and comes up with the same results as before.	To reinvestigate the problem and find a possible explanation for the performance degredation.
8			The US person suggests to the user that the problem may be at the user's end and to contact the user's Systems Administrator (SA). The user's SA looks at the performance data for the user's host, finds CPU utilization normal and indicates that there is no performance problem on the user's side.		To isolate the possible cause of the problem at the user's end.
9	System performance degrades again.	The problem occurs again, and the user calls US with the old TT reference number.	A new TT is opened and assigned to the PA as before.	The PA contacts the user's SA who looks at the user's network data to determine the activity on the network for the three time intervals that the user has reported problems. The resulting study indicates that while the network and the user's host show normal utilizations, the highest level of activity on the LAN was between the user's host and the local archive server. It is found that this traffic was due to data being transferred during a test run of an algorithm being developed by the user.	To study the network traffic for possible causes.

Table 4.1.3.2-1 User Notes Performance Degradation Scenario (3 of 3)

10	Performance degradation is recreated.	The local SA then loads a more granular peformance management product on the user's host, and with the user recreates the scenario while collecting performance data.			To test the theory that the performance degradation is caused by the interference of a test run of an algorithm.
11		It is revealed that the network adapter on the user's host is the performance bottleneck (low bandwidth), and was "choking" when the data transfer for the algorithm occurred. This was found to coincide with the time the user tried to access the Advertising Service. The SA informs the user and the personnel at the DAAC.	The TT at the DAAC is updated with the analysis & resolution and closed.		To finally resolve the problem and close the Trouble Ticket.

4.1.4 Performance Management Activities

Performance management activities include monitoring, analyzing, and reporting ECS mission and system operations, processes and component performance against pre-defined metrics. Performance metrics are set by mission objectives/priorities and system policy statements and procedure at the site and system level (SMC). Local DAAC/SMC operators use the performance management tools to collect and analyze/evaluate performance parameters associated with the DAAC's/SMC's data production and system operations management resources and processes, including network components, host operating system and peripherals, and scientific algorithm processing. At the system level, the SMC operator uses the performance management tools to collect and analyze/evaluate performance parameters associated with the system-wide ECS resources and processes, including the EBNet, SMC hosts, and DAAC host operating systems. The management process includes the application of the performance management tools to analyze local and system-wide science production and system operations trends and to modify/tune production objectives/priorities and system performance.

Performance management for the ECS system is performed by COTS and custom software tools. Software tools include local management agents residing on the individual hardware and software components of the ECS system. The primary performance management tools are the COTS products HP OpenView and Tivoli (refer to section 4.1.3 for a description of their capabilities) and a TBD math and statistical package.

Performance monitoring is done both in an on line real time mode and in an off line analysis mode. In real time, HP Openview and Tivoli monitor user selected system parameters against pre defined threshold values. An alarm is issued when values are exceeded. The capability exists to control the resetting of threshold to avoid the continuous issuing of alarms. Pre defined performance data collection profiles for performance monitoring are available on line for execution. An operator can manually define profiles tailored for special collection needs. The GUI provides a graphical interface to select and view graphs of system parameters in real-time. Periodic and asynchronous performance metrics are collected and stored in log files for further analysis. Data from local log files are automatically collected, summarized and stored into a Sybase RDMS for further evaluation. Scripts that can be manually or automatically scheduled are available to produce redefined performance reports.

Trending is performed at both the local site level and at the system level. Real time trends can be observed by viewing graphs of the current system parameters. Trend analysis can be performed by extracting historical data from local logs and the Sybase repository for analysis by the math and statistics package. Redefined scripts are available to extract data and produce both graphical and textual trending reports and projections. Projected data trends can be used to predict if and when threshold values of critical mission and system performance parameters might be reached.

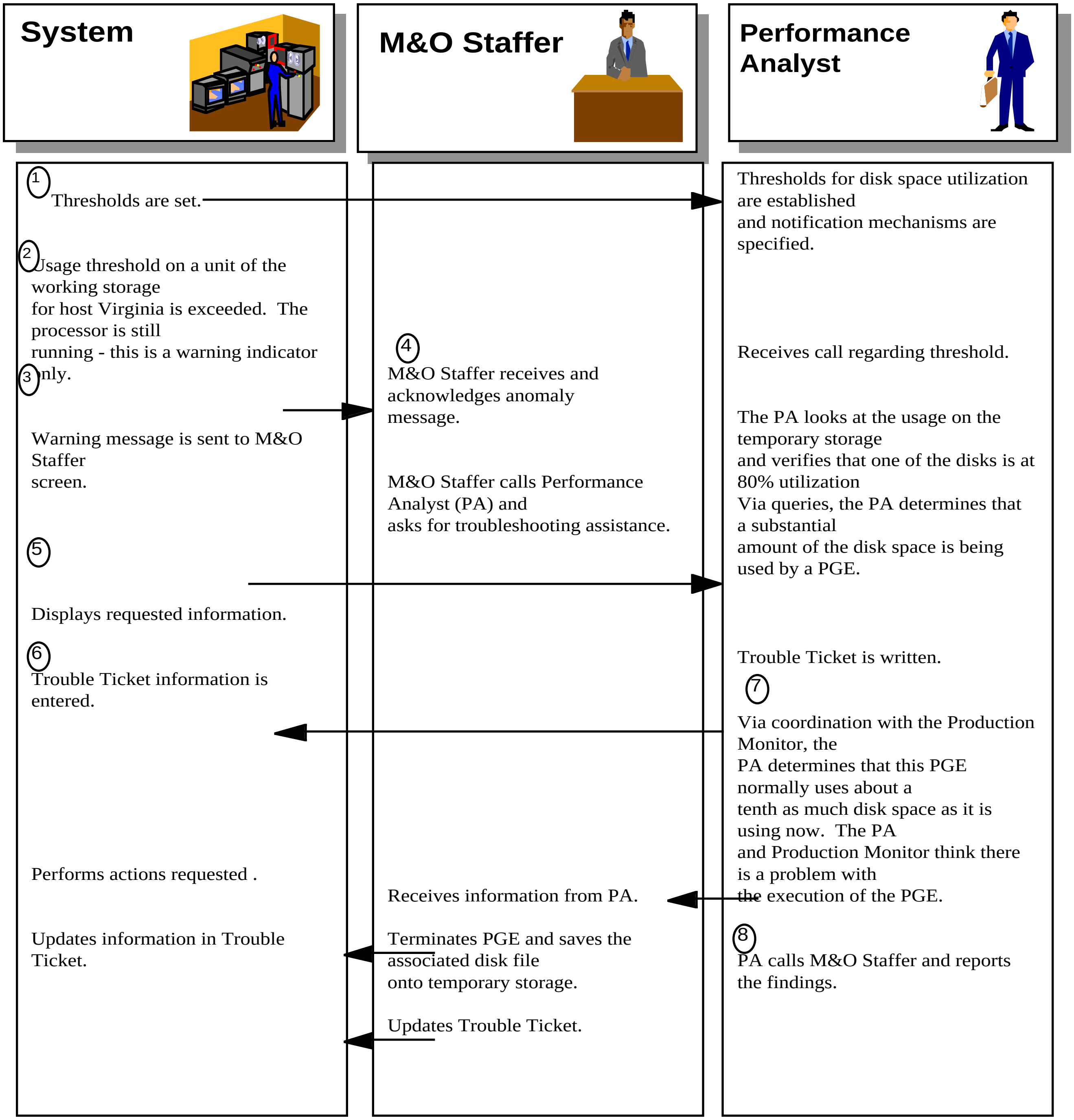
4.1.4.1 Operations Support Scenario

In this scenario, depicted in Figure 4.1.4.1- and Table 4.1.4.1-1, a problem associated with a PGE causes a large amount of disk space to be consumed. The heavy disk space utilization causes a warning to be generated, which results in the prompt identification of the faulty PGE. Prior to the beginning of the scenario, the performance analyst has already established thresholds for disk space utilization and specified notification mechanisms to be carried out in the event that those thresholds are ever exceeded.

A usage threshold on a unit of the working storage for host Virginia is exceeded. Virginia is the name of the Symmetric Multi-Processor (SMP) Science Processor at LaRC. The processor remains operational while an alert is sent to the host operator screen. The operator receives and acknowledges anomaly message. Having determined that troubleshooting assistance is required, the operator calls the performance analyst (PA) and provides him with the available information.

The PA looks at the usage on the temporary storage and verifies that one of the disks is at 80% utilization. Via queries, the PA determines that 15% of the disk resources were associated with PGE CER042197112004A (the CERES subsystem 4, Cloud Retrieval (release 2.1.)). Via further queries, the PA determines that this PGE normally uses about a tenth as much disk space as it is using now. The PA thinks there is a problem with the execution of the PGE. The PA then calls the operator and reports his findings.

The operator calls a member of the instrument team and discusses the situation with her. She suspects that the PGE has internally detected an error and has shifted to Debug mode. Under the direction of the instrument team analyst, the operator terminates the PGE, saves the associated disk file onto temporary storage and writes a Trouble Ticket.



System

1 Thresholds are set.

2 Usage threshold on a unit of the working storage for host Virginia is exceeded. The processor is still running - this is a warning indicator only.

3

Warning message is sent to M&O Staffer screen.

5

Displays requested information.

6 Trouble Ticket information is entered.

Performs actions requested .

Updates information in Trouble Ticket.

M&O Staffer

4 M&O Staffer receives and acknowledges anomaly message.

M&O Staffer calls Performance Analyst (PA) and asks for troubleshooting assistance.

Receives information from PA.

Terminates PGE and saves the associated disk file onto temporary storage.

Updates Trouble Ticket.

Performance Analyst

Thresholds for disk space utilization are established and notification mechanisms are specified.

Receives call regarding threshold.

The PA looks at the usage on the temporary storage and verifies that one of the disks is at 80% utilization Via queries, the PA determines that a substantial amount of the disk space is being used by a PGE.

Trouble Ticket is written.

7 Via coordination with the Production Monitor, the PA determines that this PGE normally uses about a tenth as much disk space as it is using now. The PA and Production Monitor think there is a problem with the execution of the PGE.

8 PA calls M&O Staffer and reports the findings.

Figure 4.1.4.1-1 Operations Support Scenario

Table 4.1.4.1-1 Operations Support Scenario (1 of 2)

Step	System	M&O Staffer	Performance Analyst	Purpose
1	Thresholds are set.		Thresholds for disk space utilization are established and notification mechanisms are specified.	To detect problems with disk space.
2	A usage threshold on a unit of the working storage for host Virginia is exceeded. Virginia is the name of the Symmetric Multi-Processor (SMP) Science Processor at LaRC. The processor is still running - this is a warning indicator only.			Recognition of threshold exceeded.
3	Warning message is sent to M&O Staffer screen.	M&O Staffer receives and acknowledges anomaly message.		To notify appropriate personnel so corrective action can be taken.
4		M&O Staffer calls Performance Analyst (PA) and asks for troubleshooting assistance.	Receives call regarding threshold.	To start the troubleshooting process.
5	Displays requested information.		The PA looks at the usage on the temporary storage and verifies that one of the disks is at 80% utilization. Via queries, the PA determines that a substantial amount of the disk is being used by PGE CER042197112004A (the CERES subsystem 4, Cloud Retrieval (release 2.1)).	To investigate the nature of the problem.
6	Trouble Ticket information entered.		Trouble Ticket written.	To log problem.
7			Via coordination with the Production Monitor, the PA determines that this PGE normally uses about a tenth as much disk space as it is using now. The PA and the Production Monitor think there is a problem with the execution of the PGE.	Evaluation of problem.

Table 4.1.4.1-1 Operations Support Scenario (2 of 2)

Step	System	M&O Staffer	Performance Analyst	Purpose
8		Receives information from PA.	PA calls M&O Staffer and reports the findings.	To apprise appropriate personnel of findings.
9	Perform actions requested (terminate PGE and save disk file).	The M&O Staffer calls an instrument team analyst and discusses the situation. The analyst suspects that the PGE has internally detected an error and has shifted to Debug mode. Under the direction of the instrument team analyst, the M&O Staffer terminates the PGE, saves the associated disk file onto temporary storage.		To enlist the help of a specialist and determine the exact cause of the problem and work out a solution.
10	Updates information in Trouble Ticket.	Updates Trouble Ticket.		Update information.

4.1.4.2 Preparing for New Algorithm Scenario

In this scenario, depicted in Figure 4.1.4.2-1 and Table 4.1.4.2-1, the planning supervisor knows that a new algorithm will be delivered in the near future and instructs the performance analyst (PA) to develop reports to allow the performance of that algorithm to be carefully monitored.

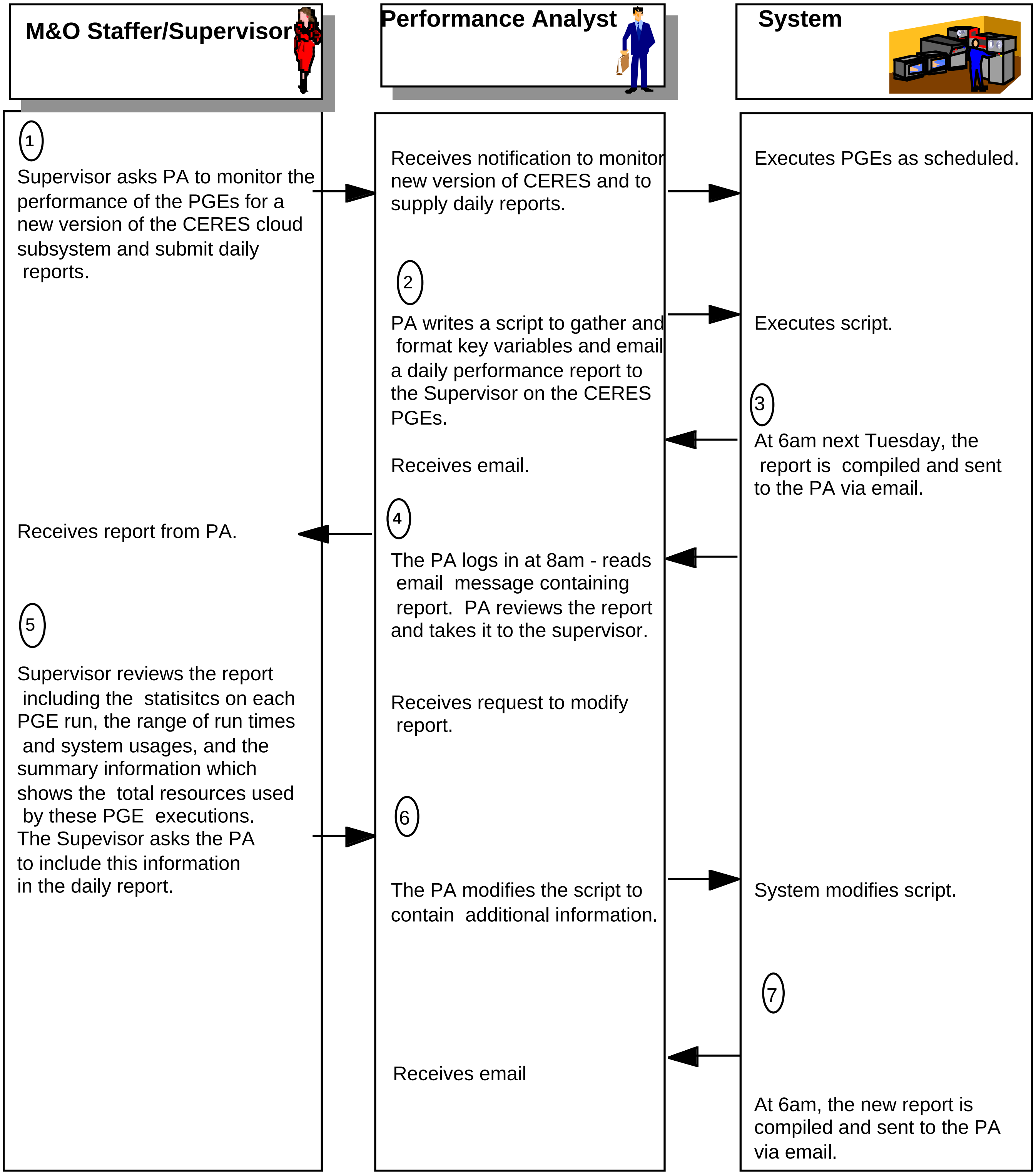
At the start of the scenario, the supervisor tells the PA that PGE’s for a new version of the CERES cloud subsystem (new clouds-during-night-time) will be executed weekly beginning next Monday morning. The supervisor asks the PA to monitor this new subsystem closely and requests daily reports on the PGE’s performance. To provide the supervisor with the requested information, the PA creates a request via a GUI to gather and format key variables and email a daily report performance report to him on the CERES specific PGE’s. The PA specifies that the report be a compilation of statistics of the last 24 hours and that the report compilation be performed at 6am daily on the day after the PGE’s run.

At 6am next Tuesday, the report is compiled and sent to the PA via email. The PA logs in at 8am and reads the email message containing the requested report. The PA reviews the report and takes it to his supervisor.

The supervisor reviews the report. She likes the statistics on each PGE run - the range of run times and system usages, and the summary information which shows the total resources used by these PGE executions. Because she also would like to know what percentage of the science processor capacity is being consumed by running these PGEs, she asks the PA to include this info in the daily report. The PA then modifies the original request to gather the additional information.

At 6am, the report is compiled and sent to the PA via email. The PA logs in at 8am and reads the email message containing the new report, including the additionally requested information. The PA takes the report to the supervisor. Upon reviewing the new report, the supervisor is pleased with the information provided. She states that the disk activity is higher than she expected, and asks for a more detailed breakdown on this. She'd like to see more information on the specific files being used, their sizes, and the types of storage they are using. Since this detail of information is not currently culled from the logs, the PA creates a script to extract the additional information from the logs and includes it in the report.

At 6am, the report is compiled and sent to the PA via email. The PA logs in at 8am and reads the email message containing the newly-revised report, including the more detailed file information requested. The PA compiles the data and takes it to the supervisor. The supervisor is pleased with information being received and asks for it to be provided to her weekly. The PA then specifies via a GUI that the data continue to be gathered daily, but that the report should be sent out weekly to both himself and his supervisor.



M&O Staffer/Supervisor

1

Supervisor asks PA to monitor the performance of the PGEs for a new version of the CERES cloud subsystem and submit daily reports.

Receives report from PA.

5

Supervisor reviews the report including the statisitcs on each PGE run, the range of run times and system usages, and the summary information which shows the total resources used by these PGE executions. The Supevisor asks the PA to include this information in the daily report.

Performance Analyst

Receives notification to monitor new version of CERES and to supply daily reports.

2

PA writes a script to gather and format key variables and email a daily performance report to the Supervisor on the CERES PGEs.

Receives email.

4

The PA logs in at 8am - reads email message containing report. PA reviews the report and takes it to the supervisor.

Receives request to modify report.

6

The PA modifies the script to contain additional information.

Receives email

System

Executes PGEs as scheduled.

Executes script.

3

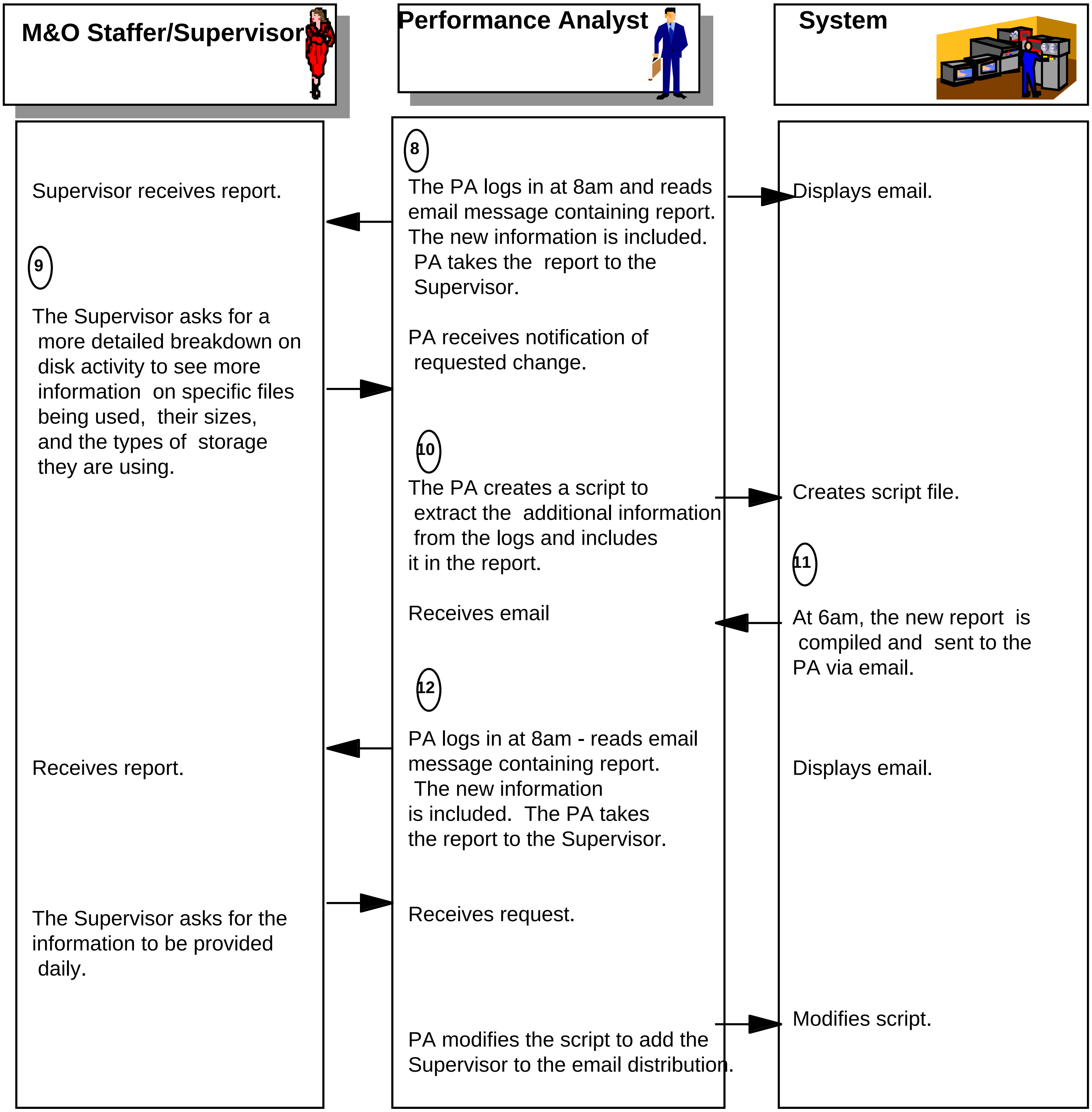
At 6am next Tuesday, the report is compiled and sent to the PA via email.

System modifies script.

7

At 6am, the new report is compiled and sent to the PA via email.

Figure 4.1.4.2-1 Preparing for New Algorithm Scenario (1 of 2)



M&O Staffer/Supervisor

Supervisor receives report.

9

The Supervisor asks for a more detailed breakdown on disk activity to see more information on specific files being used, their sizes, and the types of storage they are using.

Receives report.

The Supervisor asks for the information to be provided daily.

Performance Analyst

8

The PA logs in at 8am and reads email message containing report. The new information is included. PA takes the report to the Supervisor.

PA receives notification of requested change.

10

The PA creates a script to extract the additional information from the logs and includes it in the report.

Receives email

12

PA logs in at 8am - reads email message containing report. The new information is included. The PA takes the report to the Supervisor.

Receives request.

PA modifies the script to add the Supervisor to the email distribution.

System

Displays email.

Creates script file.

11

At 6am, the new report is compiled and sent to the PA via email.

Displays email.

Modifies script.

Figure 4.1.4.2-1 Preparing for New Algorithm Scenario (2 of 2)

Table 4.1.4.2-1 Preparing for New Algorithm Scenario (1 of 3)

Step	M&O Staffer/ Supervisor	Performance Analyst	System	Purpose
1	The M&O Staffer/Supervisor tells Performance Analyst (PA) that PGEs for a new version of the CERES cloud subsystem (new clouds-during-night-time) will be executed daily beginning next Monday morning. The supervisor asks the PA to monitor this new subsystem closely and requests daily reports on the PGE's performance.	Receives notification to monitor new version of CERES and to supply daily reports.	Executes PGE's as scheduled.	Monitor PGE's performance.
2		The PA writes a script to gather and format key variables and email a daily performance report to him on the CERES specific PGEs. The PA specifies that the report be a compilation of statistics of the last 24 hours and that the report compilation be performed at 6am daily on the day after the PGE's run.	Execute script.	To gather statistical data automatically to compile a report on the PGE's performance.
3		Receives email.	At 6am next Tuesday, the report is compiled and sent via email.	To notify PA.
4	Receives report from PA.	PA logs in at 8am - reads email message containing report. PA reviews the report and takes it to his supervisor.		To make sure the report satisfies the requirements.

Table 4.1.4.2-1 Preparing for New Algorithm Scenario (2 of 3)

Step	M&O Staffer/ Supervisor	Performance Analyst	System	Purpose
5	The M&O Staffer/Supervisor reviews the report. The statistics on each PGE run, the range of run times and system usages, and the summary information which shows the total resources used by these PGE executions. It is also desirable to know what percentage of the science processor capacity is being consumed by running these PGEs. The M&O Staffer asks the PA to include this info in the daily report.	Receives request to modify report.		To notify the supervisor.
6		PA modifies the script to gather the additional information.	Modifies script.	To gather additional information for the report.
7			At 6am, the report is compiled and sent to the PA via email.	To notify the PA.
8	Receives report.	PA logs in at 8am and reads email message containing report. The new information is included. The PA takes the report to the supervisor.	Displays email.	To notify the M&O Staffer/Supervisor.
9	The M&O Staff/Supervisor is pleased with the new report. The M&O Staffer states that the disk activity is higher than expected, and asks for a more detailed breakdown on this. The M&O Staffer would like to see more information on the specific files being used, their sizes, and the types of storage they are using.	PA receives notification of requested change.		To identify what kind of files are being used, what their sizes are, and what types of storage they are using.

Table 4.1.4.2-1 Preparing for New Algorithm Scenario (3 of 3)

Step	M&O Staffer/ Supervisor	Performance Analyst	System	Purpose
10		Since this detail of information is not currently culled from the logs, the PA creates a script to extract the additional information from the logs and includes it in the report. Note: Historical log data may be retrieved from the Data Archive. Archived data may be retrieved over an operator-specified time period (e.g., for a specified day or week).	Creates script file.	To retrieve more detailed information from the logs.
11			At 6am, the new report is compiled and sent to the PA via email.	To notify the PA.
12	Receives Report.	PA logs in at 8am and reads email message containing the report. The new information is included. PA takes the report to the supervisor.	Displays email.	To notify the M&O Staffer/Supervisor.
13	The M&O Staffer/Supervisor is pleased with the information being received and asks for it to be provided daily.	Receives request.		To retrieve detailed info daily.
14		PA modifies the script to add the M&O Staffer/Supervisor to the email distribution.	Modifies script.	To inform M&O Staffer of report the same time as PA.

4.1.4.3 Trending Scenario

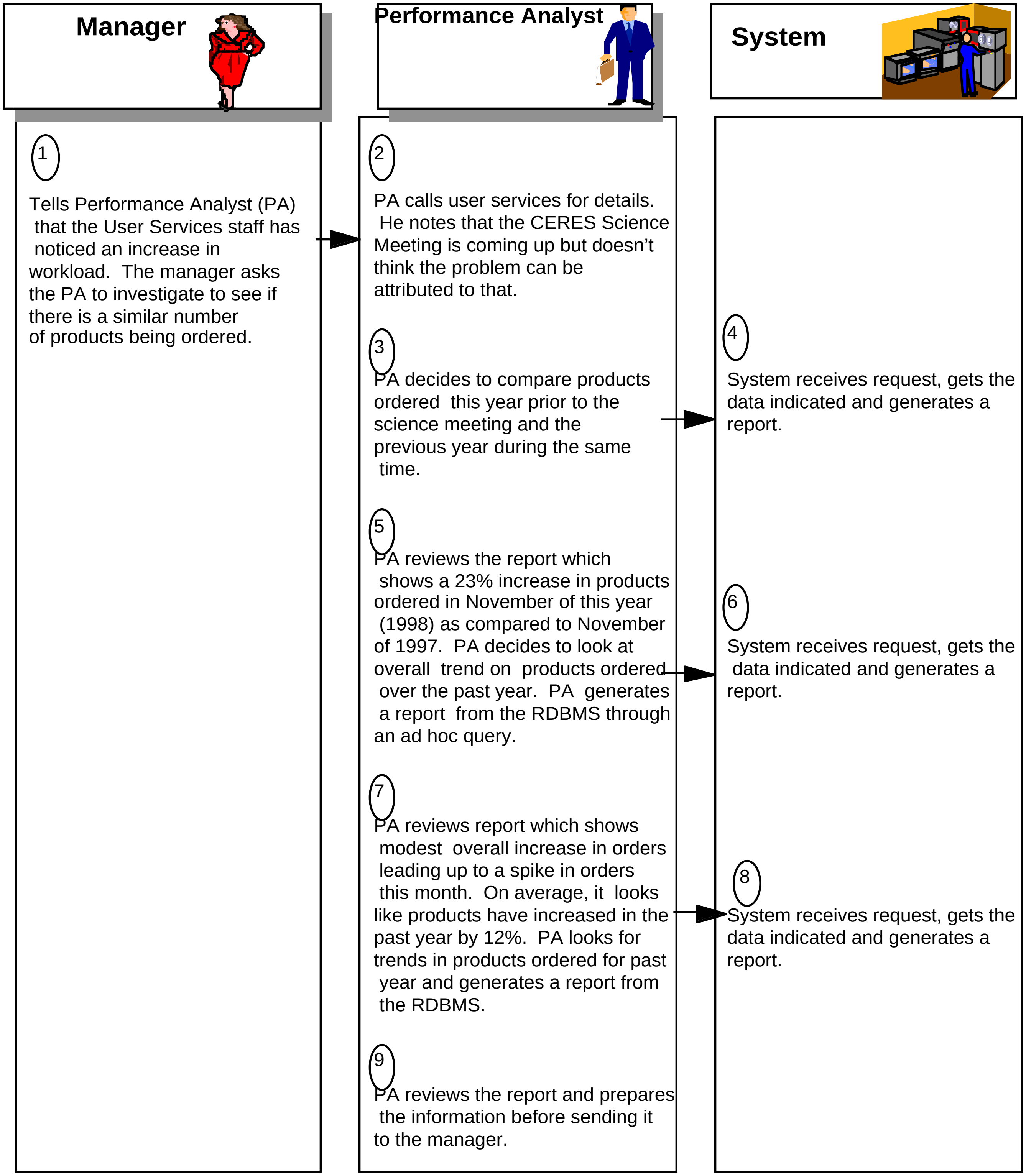
In this scenario, depicted in Figure 4.1.4.3-1 and Table 4.1.4.3-1, the load on the system, in terms of the number of products ordered, is analyzed to determine any long term trends. This analysis is important to help predict the need for system upgrades to meet user requirements.

The scenario begins when the performance analyst (PA) is informed by his supervisor that the User Services staff has indicated that their workload has increased - lots of users are calling with questions - many are new to the DAAC. She asks PA to investigate and see if there is a similar increase in the number of products being ordered. The PA calls user services (US) to get more details. The US person agrees that things seem busier. He notes that the CERES Science Meeting is coming up next month (December 1998), but that he doesn't think it can all be attributed to that.

The PA decides to first look at the comparison of the products ordered this year prior to the science meeting and last year during the same time. The PA generates a report from the RDBMS through an ad hoc data query. The report generator receives the request, gets the data indicated and generates a report. Upon receiving the report, the PA notices that it shows a 23% increase in products ordered in November of this year (1998) as compared to November of 1997. The PA then decides to look at the overall trend on products ordered over the past year.

The PA generates a new report from the RDBMS via an ad hoc query. The report generator receives the request, gets the data indicated and generates a report. Upon reviewing this report, the PA notices that there has been a modest overall increase in orders leading up to a spike in orders this month (for the meeting). On average, it looks like product orders have increased in the past year by 12%.

The PA then decides to look at the types of products ordered in the past year to look for trends and generates a report from the RDBMS through an ad hoc query. The report generator receives the request, gets the data indicated and generates a report. On reviewing this report, the PA notices that it indicates a mixed bag of information - some products (i.e., CER08 - Level 3 monthly regional radiative fluxes and clouds, and CER15 - Level 3 monthly zonal and global radiative fluxes and clouds) are being ordered more, but orders for others (i.e., CER14 - Level 3 ERBE-like monthly gridded average) have actually decreased. The PA then prepares all of this information into a report and presents it to the manager for possible further action.



Manager

Performance Analyst

System

1 Tells Performance Analyst (PA) that the User Services staff has noticed an increase in workload. The manager asks the PA to investigate to see if there is a similar number of products being ordered.

2 PA calls user services for details. He notes that the CERES Science Meeting is coming up but doesn't think the problem can be attributed to that.

3 PA decides to compare products ordered this year prior to the science meeting and the previous year during the same time.

4 System receives request, gets the data indicated and generates a report.

5 PA reviews the report which shows a 23% increase in products ordered in November of this year (1998) as compared to November of 1997. PA decides to look at overall trend on products ordered over the past year. PA generates a report from the RDBMS through an ad hoc query.

6 System receives request, gets the data indicated and generates a report.

7 PA reviews report which shows modest overall increase in orders leading up to a spike in orders this month. On average, it looks like products have increased in the past year by 12%. PA looks for trends in products ordered for past year and generates a report from the RDBMS.

8 System receives request, gets the data indicated and generates a report.

9 PA reviews the report and prepares the information before sending it to the manager.

Figure 4.1.4.3-1 Trending Scenario

Table 4.1.4.3-1 Trending Scenario (1 of 2)

Step	Manager	Performance Analyst	System	Purpose
1	Tells Performance Analyst (PA) that the User Services staff has indicated that their workload has increased - lots of users are calling with questions - many are new to the DAAC. She asks PA to investigate and see if there is a similar increase in the number of products being ordered.			To investigate the recent workload increase.
2		PA calls user services to get more details. The US person agrees that things seem busier. He notes that the CERES Science Meeting is coming up next month (December 1998), but that he doesn't think it can all be attributed to that.		
3		PA decides to first look at the comparison of the products ordered this year prior to the science meeting and the previous year during the same time. PA generates a report from the RDBMS through an ad hoc query.		To determine if the increased workload may be attributed to upcoming CERES Science Meeting.
4			System receives request, gets the data indicated and generates a report.	
5		PA reviews the report. It shows a 23% increase in products ordered in November of this year (1998) as compared to November of 1997. PA then decides to look at the overall trend on products ordered over the past year. PA generates a report from the RDBMS through an ad hoc query.		To perform trend analysis in an effort to find a correlation between an increase in products ordered and an increase in workload.
6			System receives request, gets the data indicated and generates a report.	

Table 4.1.4.3-1 Trending Scenario (2 of 2)

Step	Manager	Performance Analyst	System	Purpose
7		PA reviews the report. It shows a modest overall increase in orders leading up to a spike in orders this month (for the meeting). On average, it looks like product orders have increased in the past year by 12%. PA then decides to look at the types of products ordered in the past year to look for trends. PA generates a report from the RDBMS through an ad hoc query.		To determine other possible causes for the increase in workload.
8			System receives request, gets the data indicated and generates a report.	
9		PA reviews the report. It indicates a mixed bag of information - some products (i.e., CER08 - Level 3 monthly regional radiative fluxes and clouds, and CER15 - Level 3 monthly zonal and global radiative fluxes and clouds) are being ordered more, but orders for others (i.e., CER 14 - Level 3 ERBE - like monthly gridded average) have actually decreased. PA prepares this information into a report and presents it to the manager.		To look at the data in the trending report and understand the cause of the increased workload.

4.1.4.4 Performance Test Generation Request Scenario

See Figure 4.1.4.4-1 for a pictorial representation and Table 4.1.4.4-1 for a sequence of events for the Performance Test Generation Request Scenario.

This scenario involves the installation of a new algorithm on a host. The Resource Manager must ensure that the performance of the host containing the new algorithm will continue to perform within the DAAC policy specifications.

Via E-Mail, the Resource Manager notifies the Performance Analyst (PA) to develop and schedule performance tests to monitor the host's performance following the algorithm's installation and to verify system compliance with performance metrics. From his console, the PA retrieves a copy of the DAAC Resource Schedule to determine when the new algorithm is scheduled to be installed. The PA also retrieves a copy of the DAAC performance policy instructions to determine the desired performance metrics for the specified host. He saves a copy for his future reference and e-mails a copy to the Resource Manager.

From the policy instructions, the PA determines that performance data needs to be collected during normal system operations over at least 3 non-weekend days following the algorithm installation. Policy also states that test periods should be a minimum of 12 contiguous hours covering peak usage times and should be free of interference from other tests, training, simulations or system maintenance.

The PA reviews the ground event schedule and determines that the new algorithm is being installed and tested Sunday. He determines that there are no currently scheduled special ground events on the following Monday, Tuesday and Wednesday. The PA then submits a Resource Request to the Resource Planner to add the performance tests to the Site Resource Schedule by specifying the host and a test name and sets the start and end times from 6 AM to 6 PM on Monday, Tuesday and Wednesday. As the algorithm change has a potential impact on operations, he requests a high priority. To further clarify the new events, a note is added stating the test purpose and expected results and stating that no other special events should be scheduled on the host during the test duration. As the tests to be performed are non- intrusive, it is further stated that there are no expected impacts to normal operations due to the test activity. The Resource Request is processed and approved.

From the system management console, the PA displays a list of previously defined performance profiles. A profile is identified that collects the metrics specified in the policy instructions.

Using the collection metrics specified in policy instructions, the PA modifies the selected performance profile by activating the collection of all parameters specified for collection. Next, the sample frequency rates are set to the specified levels, and the daily times for collection are set. As this is a test of normal system operations, the log file name remains as the standard file name being used to collect sample performance data. Finally, the modified profile is scheduled for dissemination to the host computer at 5 AM Monday morning.

From the system management console, the PA again displays a list of previously defined performance profiles. The PA selects the profile designed for normal performance monitoring and schedules it for dissemination to the host at 6 PM Wednesday to return performance collection to its nominal state. The PA also displays a list of previously defined scripts for report generation. The PA identifies a script to produce a report on the metrics as specified in the policy instructions. The PA schedules the script to be executed after 6 PM on the following Monday, Tuesday, and Wednesday and specifies that the resulting report be E-mailed to himself and the Resource Manager.

Upon receiving the three daily performance reports, the PA and Resource Manager compare the generated metrics against the nominal values specified in the DAAC performance policy instructions. Values are determined to be within the policy guidelines. The PA notifies the Resource Manager by E-Mail that the new algorithm is performing within specifications. The Resource Manager reports the results to management

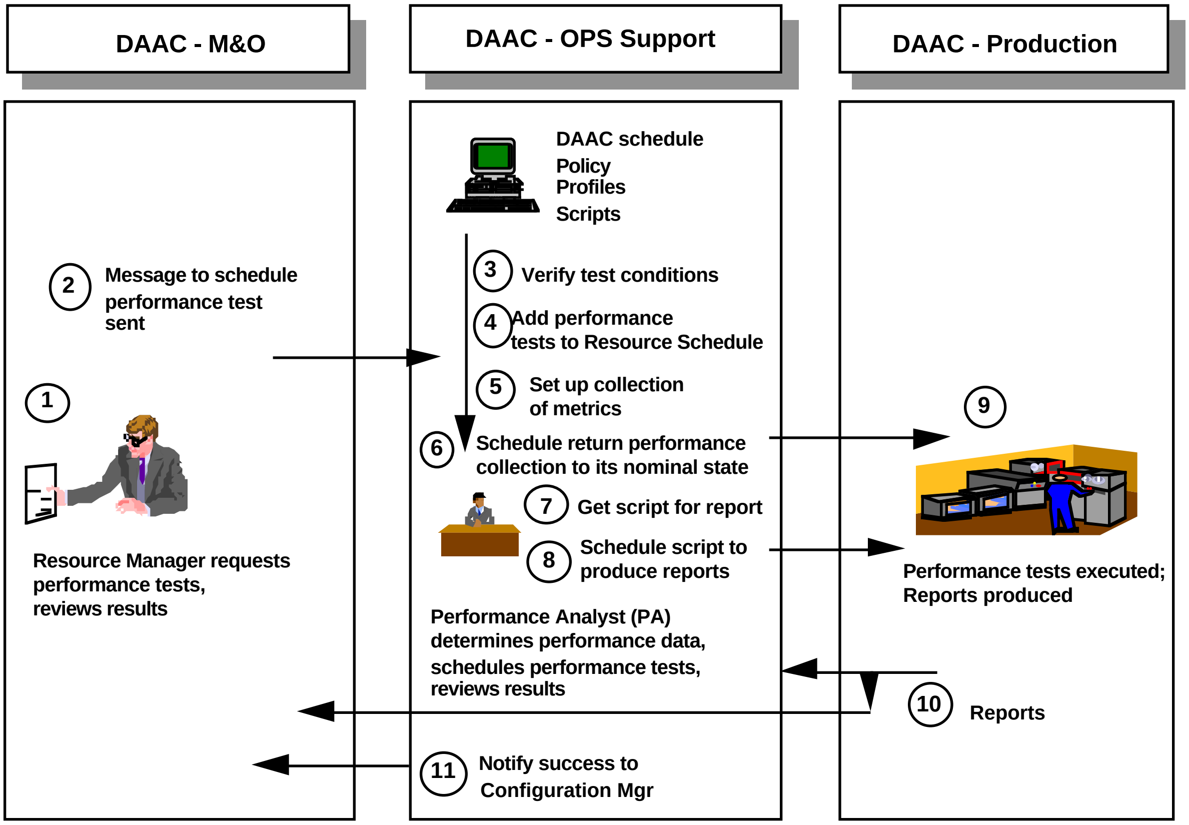

DAAC - M&O
DAAC - OPS Support
DAAC - Production
DAAC schedule
Policy
Profiles
Scripts
2
Message to schedule performance test sent
3
Verify test conditions
4
Add performance tests to Resource Schedule
5
Set up collection of metrics
1
6
Schedule return performance collection to its nominal state
9
7
Get script for report
8
Schedule script to produce reports
Resource Manager requests performance tests, reviews results
Performance tests executed; Reports produced
Performance Analyst (PA) determines performance data, schedules performance tests, reviews results
10
Reports
11
Notify success to Configuration Mgr

Figure 4.1.4.4-1. Performance Test Generation Scenario

Table 4.1.4.4-1. Steps of the Scenario: Performance Test Generation (1 of 2)

Scenario Assumptions: The DAAC performance policy instructions specify that performance data needs to be collected during normal system operations over at least 3 non-weekend days following the installation of a new algorithm. Policy also states that test periods should be a minimum of 12 contiguous hours covering peak usage times and should be free of interference from other tests, training, simulations or system maintenance. The purpose of this scenario is to insure that the performance of the host containing a new algorithm will continue to perform within DAAC policy specifications.

Step	Operator/User	System	Purpose
1	The Resource Manager determines that performance tests need to be run to monitor a host's performance following the installation of a new algorithm.		Insure nominal host performance.
2	Resource Manager notifies the Performance Analyst (PA) to develop and schedule tests to verify system compliance.	E-Mail message from Resource Manager transmitted to PA.	Determine conditions and metrics for test.

Table 4.1.4.4-1. Steps of the Scenario: Performance Test Generation (2 of 2)

Step	Operator/User	System	Purpose
3	PA reviews the ground event schedule and determines that the new algorithm is being installed and tested Sunday. He determines that there are no currently scheduled special ground events on the following Monday, Tuesday, and Wednesday.	System displays Resource Schedule with start and stop times.	Verify test conditions.
4	PA submits Resource Request to add the performance tests to the Resource Schedule. Start and end times are set from 6 AM to 6 PM on Monday, Tuesday, and Wednesday. Algorithm is assigned a high priority. Test purpose and expected results are noted.	Performance test times are set.	Set up performance tests.
5	The PA displays a list of previously defined performance profiles. A profile is identified that collects the metrics specified in the policy instructions. The profile is modified and scheduled.	Displays profile list. Modifies profile to PA's specification. Schedules dissemination of test profile.	Set up collection of performance metrics.
6	PA selects the profile designed for normal performance monitoring and schedules it for dissemination to host at 6 PM Wednesday.	Dissemination of nominal profile is scheduled.	Return performance collection to its nominal state after test.
7	PA requests the displays of a list of scripts for report generation. Identifies script to produce a report on the metrics per policy instructions.	List of scripts displayed.	Produce a report on the metrics.
8	PA schedules the script to be executed after 6 PM on the following Monday, Tuesday, and Wednesday and specifies that the resulting report be e-mailed to himself and the Resource Manager.	Performance reports are scheduled.	Produce reports of performance at specified times.
9		System performs test without incident on Mon., Tue., Wed.	Performance Analysis
10	The PA and Resource Manager review reports.	Sends reports.	Verify system performance.
11	The PA notifies the Resource Manager of success by E-Mail.	E-Mail messages sent.	Conclude testing.

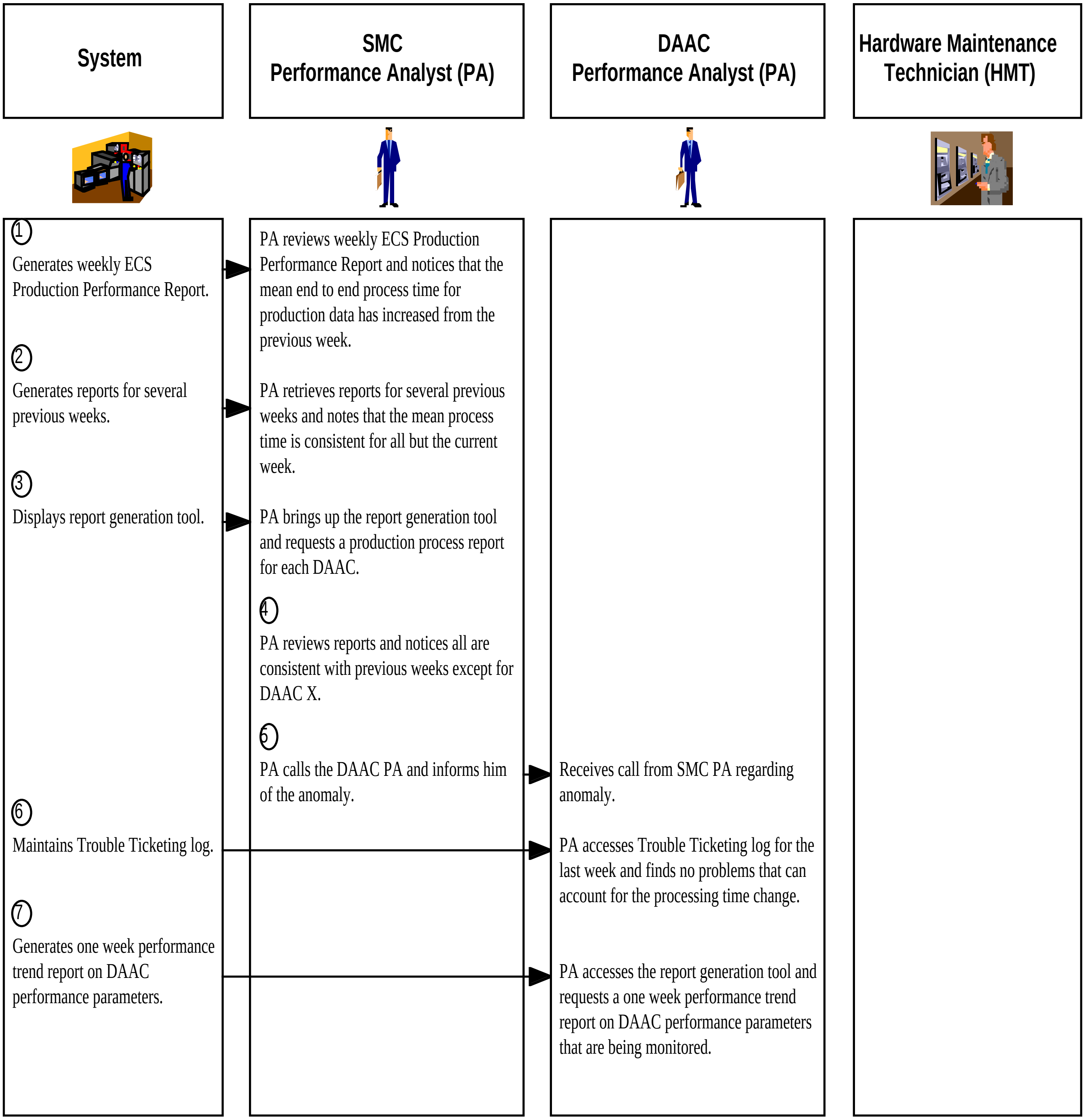
4.1.4.5 Cross DAAC Problem Detection Scenario

In this scenario, a Performance Analyst (PA) stationed at the SMC examines the weekly ECS Production Performance Report and notices that the mean end to end process time for production data has increased from the previous week. In order to better understand the situation, the SMC PA retrieves reports for several previous weeks and notes that the mean process time is consistent for all but the current week. Next, the Performance Analyst brings up the report generation tool and requests a production process report for each DAAC. Upon review of the reports, the Performance Analyst notices that all reports are consistent with previous weeks except for DAAC X. The SMC Performance Analyst calls the DAAC Performance Analyst and informs him of the anomaly. The DAAC PA accesses the Trouble Ticketing log for the last week and finds no problems that can account for the processing time change. The DAAC PA then accesses the report generation tool and requests a one week performance trend report on DAAC performance parameters that are being monitored. Upon review of the performance parameter trends, the DAAC PA finds that the MIB object "tcpRetransSegs" for the FDDI switch shows a periodic increase in the total number of segments being transmitted but not enough of an increase to pass the threshold value currently set for the object. The DAAC PA then writes a Trouble Ticket for the FDDI switch. Afterwards, the DAAC PA calls the SMC PA and informs him of the possible cause and that a Trouble Ticket has been written.

From the system management console, the DAAC PA accesses Tivoli and displays the performance profile for the FDDI switch. He then lowers the threshold setting for the "tcpRetransSegs" MIB object to detect the upper limits reached during the previous week.

The Hardware Maintenance Technician (HMT) runs diagnostics on the FDDI switch and finds and repairs a hardware problem. He then closes the Trouble Ticket.

The next week, the PA at the SMC reviews the weekly ECS Production Performance Report and observes that the mean end-to-end process time for production data has returned to its nominal value of the prior weeks. The SMC PA calls the DAAC PA and informs him that the problem appears to be accounted for and corrected.



System

SMC Performance Analyst (PA)

DAAC Performance Analyst (PA)

Hardware Maintenance Technician (HMT)

1 Generates weekly ECS Production Performance Report.

PA reviews weekly ECS Production Performance Report and notices that the mean end to end process time for production data has increased from the previous week.

2 Generates reports for several previous weeks.

PA retrieves reports for several previous weeks and notes that the mean process time is consistent for all but the current week.

3 Displays report generation tool.

PA brings up the report generation tool and requests a production process report for each DAAC.

4 PA reviews reports and notices all are consistent with previous weeks except for DAAC X.

5 PA calls the DAAC PA and informs him of the anomaly.

Receives call from SMC PA regarding anomaly.

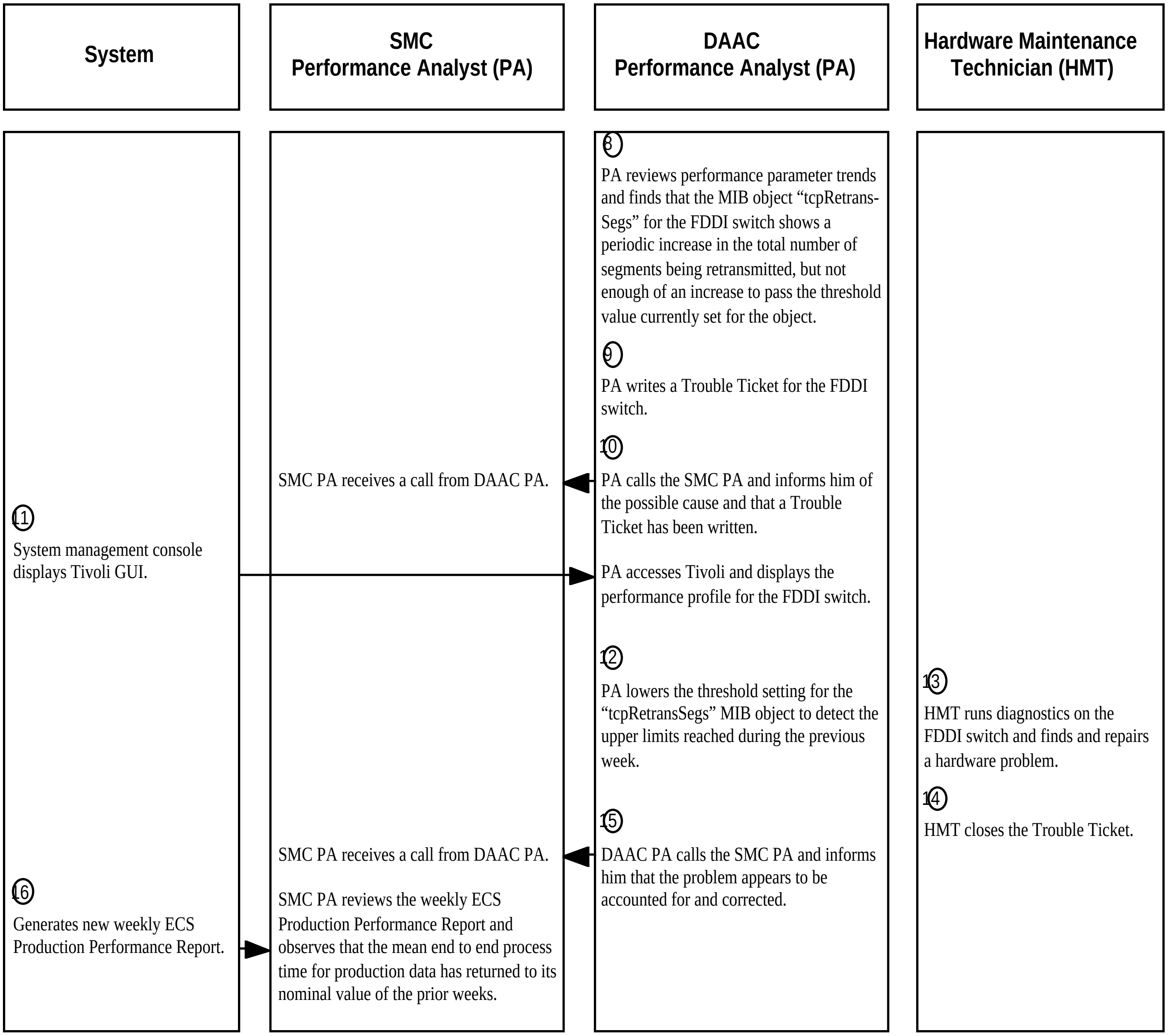
6 Maintains Trouble Ticketing log.

PA accesses Trouble Ticketing log for the last week and finds no problems that can account for the processing time change.

7 Generates one week performance trend report on DAAC performance parameters.

PA accesses the report generation tool and requests a one week performance trend report on DAAC performance parameters that are being monitored.

Figure 4.1.4.5-1 Cross DAAC Problem Detection Scenario (1 of 2)


System
SMC Performance Analyst (PA)
DAAC Performance Analyst (PA)
Hardware Maintenance Technician (HMT)

8 PA reviews performance parameter trends and finds that the MIB object “tcpRetrans-Segs” for the FDDI switch shows a periodic increase in the total number of segments being retransmitted, but not enough of an increase to pass the threshold value currently set for the object.

9 PA writes a Trouble Ticket for the FDDI switch.

10 PA calls the SMC PA and informs him of the possible cause and that a Trouble Ticket has been written.

SMC PA receives a call from DAAC PA.

11 System management console displays Tivoli GUI.

PA accesses Tivoli and displays the performance profile for the FDDI switch.

12 PA lowers the threshold setting for the “tcpRetransSegs” MIB object to detect the upper limits reached during the previous week.

13 HMT runs diagnostics on the FDDI switch and finds and repairs a hardware problem.

14 HMT closes the Trouble Ticket.

15 DAAC PA calls the SMC PA and informs him that the problem appears to be accounted for and corrected.

SMC PA receives a call from DAAC PA.

16 Generates new weekly ECS Production Performance Report.

SMC PA reviews the weekly ECS Production Performance Report and observes that the mean end to end process time for production data has returned to its nominal value of the prior weeks.

Figure 4.1.4.5-1 Cross DAAC Problem Detection Scenario (2 of 2)

Table 4.1.4.5-1 Cross DAAC Problem Detection Scenario (1 of 3)

Step	System	SMC Performance Analyst	DAAC Performance Analyst	Hardware Maintenance Technician (HMT)	Purpose
1	Generates weekly ECS Production Performance Report.	The Performance Analyst (PA) at the SMC reviews the weekly ECS Production Performance Report and notices that the mean end to end process time for production data has increased from the previous week.			To determine the status of Production Performance.
2	Generates Production Performance Reports for several previous weeks.	The PA retrieves reports for several previous weeks and notes that the mean process time is consistent for all but the current week.			To compare the current weekly report with previous reports and determine if any discrepancies exist.
3	Displays report generation tool.	The PA brings up the report generation tool and requests a production process report for each DAAC.			To compare production performance at each DAAC.
4		The PA reviews the reports and notices that all are consistent with previous weeks except for DAAC X.			To isolate any potential problems.
5		The SMC PA calls the DAAC PA and informs him of the anomaly.	Receives call from SMC PA regarding anomaly.		To notify DAAC PA of a possible problem.
6	Retrieves Trouble Ticketing log.		The DAAC PA accesses the Trouble Ticketing log for the last week and finds no problems that can account for the processing time change.		To determine if a Trouble Ticket was written that could account for the processing time change.
7	Generates one week performance trend report on DAAC performance parameters.		The DAAC PA accesses the report generation tool and requests a one week performance trend report on DAAC performance parameters that are being monitored.		To evaluate performance trending on DAAC performance parameters.

Table 4.1.4.5-1 Cross DAAC Problem Detection Scenario (2 of 3)

Step	System	SMC Performance Analyst	DAAC Performance Analyst	Hardware Maintenance Technician (HMT)	Purpose
8			The DAAC PA reviews the performance parameter trends and finds that the MIB object "tcpRetransSegs" for the FDDI switch shows a periodic increase in the total number of segments being retransmitted, but not enough of an increase to pass the threshold value currently set for the object.		To locate a possible explanation for the anomaly.
9			The DAAC PA writes a Trouble Ticket for the FDDI switch.		To evaluate FIDDI switch for possible problem.
10		Receives call from DAAC PA.	The DAAC PA calls the SMC PA and informs him of the possible cause and that a Trouble Ticket has been written.		To make the SMC PA aware of the situation.
11	System management console displays Tivoli GUI.		From the system management console, the DAAC PA accesses Tivoli and displays the performance profile for the FDDI switch.		To review performance profile for the FIDDI switch.
12			The DAAC PA lowers the threshold setting for the "tcpRetransSegs" MIB object to detect the upper limits reached during the previous week.		For system to send trap if MIB object value reaches levels of last week.

Table 4.1.4.5-1 Cross DAAC Problem Detection Scenario (3 of 3)

Step	System	SMC Performance Analyst	DAAC Performance Analyst	Hardware Maintenance Technician (HMT)	Purpose
13				The Hardware Maintenance Technician (HMT) runs diagnostics on the FDDI switch and finds and repairs a hardware problem.	To determine the cause of the problem and correct it.
14				The HMT closes the Trouble Ticket.	To indicate that the problem has been resolved.
15		The SMC PA reveices a call from the DAAC PA.	The DAAC PA calls the SMC PA and informs him that the problem appears to be accounted for and corrected.		To inform SMC PA that a problem has been identified.
16	Generates new weekly ECS Production Performance Report.	The next week, the SMC PA reviews the weekly ECS Production Performance Report and observes that the mean end to end process time for production data has returned to its nominal value of the prior weeks.			To determine the status on the mean end to end process time for production data and verify that problem has been found.